Advanced Linear Algebra

Manfred Kolster
with revisions by *Romyar Sharifi*

Contents

CHAPTER 1

ALGEBRAIC BACKGROUND

1. Fields

In an introductory linear algebra course, one generally considers vector spaces for which the scalars are real numbers. The vast majority of the results that you may have seen for *real* vector spaces remain unchanged if we allow other systems of numbers as scalars, as long as they form a *field*. Fields are defined by generalizing the essential algebraic properties of the real numbers in the same way an abstract real vector space generalizes $\mathbb{R}^n$. That is to say, we can axiomatize the properties of the real numbers so that they become a single example of a larger class of fields. We can consider vector spaces over a field satisfying the same axioms as real vector spaces, except that the scalars are elements of the new field.

Let us analyze the properties of fields. We start with two "compositions": "$+$" and "$\cdot$". With respect to each of these compositions the underlying structure is that of a *group*, which is formally defined as follows:

DEFINITION 1.1. A nonempty set G with a composition $\circ$ is a **group** if

1. $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$ (**associativity**).

2. There exists an **identity element** e in G such that $e \circ a = a \circ e = a$ for all $a \in G$.

3. For each $a \in G$, there exists an **inverse** a^{-1} in G such that

$$a \circ a^{-1} = a^{-1} \circ a = e.$$

If, in addition, the composition $\circ$ is **commutative**, i.e.,

4. $a \circ b = b \circ a$ for all $a, b \in G$,

then G is called **abelian**.

Groups are the fundamental building blocks for most algebraic structures. Here are some examples:

EXAMPLES 1.2. a. The real numbers $\mathbb{R}$ form a group under addition. The nonzero real numbers $\mathbb{R} \setminus \{0\}$ form a group under multiplication.

b. The complex numbers $\mathbb{C}$ from a group under addition. The nonzero complex numbers $\mathbb{C} \setminus \{0\}$ form a group under multiplication.

c. The integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ form a group under addition.

All these groups are abelian groups, and most of the groups we deal with will be abelian. However, nonabelian groups certainly exist, and here are a few examples:

d. The set of real invertible $n \times n$-matrices forms a group under multiplication, the **general linear group** $GL_n(\mathbb{R})$. This group is nonabelian for $n \geq 2$.

e. The subset of $GL_n(\mathbb{R})$ of all matrices with determinant 1 forms a group under multiplication, the **special linear group** $SL_n(\mathbb{R})$. Again, this group is nonabelian for $n \geq 2$.

f. The set of possible moves (rotations of faces) on a Rubik's cube forms a nonabelian group under composition.

Axioms 2 and 3 in the definition of a group suggest that the identity element and the inverse are uniquely determined, which is in fact true, but needs a proof:

LEMMA 1.3. *Let G be a group.*

i. If

$$a \circ e = e \circ a = a \quad \textit{and} \quad a \circ e' = e' \circ a = a$$

for all $a \in G$, then $e = e'$.

ii. If

$$a \circ b = b \circ a = e \quad \textit{and} \quad a \circ c = c \circ a = e,$$

then $b = c$.

PROOF. i. Using the properties of e and e', we have

$$e' = e' \circ e = e.$$

ii. We have

$$b = b \circ e = b \circ (a \circ c) = (b \circ a) \circ c = e \circ c = c.$$

□

Here are two properties valid in an arbitrary group G:

LEMMA 1.4. *Let G be a group with composition $\circ$.*

i. (Cancellation) If $a \circ b = a \circ c$ or $b \circ a = c \circ a$, then $b = c$.

ii. For any given $a, b \in G$, the equation $a \circ x = b$ has the unique solution $x = a^{-1} \circ b$.

PROOF. i. Assume that $a \circ b = a \circ c$. We have

$$b = e \circ b = (a^{-1} \circ a) \circ b = a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c) = (a^{-1} \circ a) \circ c = e \circ c = c.$$

The other case is similar.

ii. We have

$$x = e \circ x = (a^{-1} \circ a) \circ x = a^{-1} \circ (a \circ x) = a^{-1} \circ b.$$

□

We have seen in Examples 1.2a and b that $\mathbb{R}$ and $\mathbb{C}$ have two underlying group structures with respect to addition and multiplication. We also know that addition and multiplication are linked via distributivity. These properties now lead to the general definition of a field.

DEFINITION 1.5. A **field** F is a nonempty set with two operations $+$ and $\cdot$ satisfying the following list of properties. Note: it is common to simply write ab instead of $a \cdot b$ for the product of two elements a, b in F.

1. F is an abelian group with respect to addition. Its identity element is called 0, and the additive inverse of $x \in F$ is denoted $-x$.

2. $F \setminus \{0\}$ is an abelian group with respect to multiplication. Its identity element is called 1, and the multiplicative inverse of $x \in F \setminus \{0\}$ is denoted x^{-1}.

3. $a(b + c) = ab + ac$ for all $a, b, c \in F$ (*distributivity*).

Of course, $\mathbb{R}$ and $\mathbb{C}$ are fields, but we also see that the set $\mathbb{Q}$ of rational numbers is a field.

Here are a few essential properties of a field F derived from the use of the distributivity law:

LEMMA 1.6. *Let F be a field. The following statements hold:*

i. $ab = 0 \Longleftrightarrow a = 0$ *or* $b = 0$.

ii. $(-1)a = -a$ *for all* $a \in F$.

PROOF. i. We first note that

$$0\,b = (0 + 0)b = 0\,b + 0\,b.$$

Cancellation implies $0\,b = 0$ for all $b \in F$. Let us assume now that $ab = 0$ and that $a \neq 0$. We have to show that $b = 0$. Now

$$ab = 0 = a\,0.$$

Since $a \neq 0$, we can cancel a and obtain $b = 0$, as claimed.

ii. We have

$$0 = 0\,a = (1 + (-1))a = a + (-1)a.$$

On the other hand $0 = a + (-a)$, which proves the claim.

□

To obtain some more examples of fields, in fact, fields with only finitely many elements, we start with the set of integers $\mathbb{Z}$, which is **not** a field. If n is any fixed positive integer > 1, then we can divide any other integer m by n with a remainder r between 0 and $n - 1$:

$$m = qn + r, \quad q \in \mathbb{Z}, \quad 0 \leq r \leq n - 1.$$

This is called the **Division Algorithm**. We denote the remainder r of m upon division by n by $\overline{m}$. We note that

$$\overline{m_1} = \overline{m_2} \Longleftrightarrow n \mid (m_1 - m_2).$$

The set of the possible remainders, or **integers modulo n**, is denoted by $\mathbb{Z}/n\mathbb{Z}$:

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Given any element $\overline{i} \in \mathbb{Z}/n\mathbb{Z}$, there are infinitely many integers m for which $\overline{m} = \overline{i}$, namely all m of the form

$$m = qn + i, \quad q \in \mathbb{Z}.$$

We call m a representative of $\bar{i}$ if $\overline{m} = \bar{i}$.

EXAMPLE 1.7. Let us take $n = 2$. Then $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$. An integer m represents $\bar{0}$ if and only if m is even, and it represents $\bar{1}$ if and only if m is odd.

We want to define addition and multiplication on the set $\mathbb{Z}/n\mathbb{Z}$ as follows:

$$\overline{m_1} + \overline{m_2} = \overline{m_1 + m_2}$$

and

$$\overline{m_1} \cdot \overline{m_2} = \overline{m_1 m_2}.$$

There is a little problem with this definition because we are using representatives, and therefore we have to show that the definition is independent of the choice of representatives. In mathematical terminology, we have to show that addition and multiplication are *well-defined*.

Assume then that $\overline{m_1} = \overline{m_1'}$ and $\overline{m_2} = \overline{m_1'}$. We have

$$m_1' = m_1 + q_1 n \quad \text{and} \quad m_2' = m_2 + q_2 n,$$

and we obtain

$$m_1' + m_2' = m_1 + m_2 + (q_1 + q_2)n \quad \text{and} \quad m_1' m_2' = m_1 m_2 + (m_1 q_2 + m_2 q_1 + q_1 q_2)n,$$

which indeed shows that

$$\overline{m_1' + m_2'} = \overline{m_1 + m_2} \quad \text{and} \quad \overline{m_1' m_2'} = \overline{m_1 m_2}.$$

Therefore, addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ are well-defined. It should be clear now from the very definition of addition and multiplication that the set $\mathbb{Z}/n\mathbb{Z}$ inherits all the properties of $\mathbb{Z}$. In particular, $\mathbb{Z}/n\mathbb{Z}$ is an abelian group with respect to addition, the identity element being $\bar{0}$ and the inverse of $\bar{i}$ being $\overline{-i} = \overline{n - i}$. Furthermore, distributivity holds and $\bar{1}$ plays the role of 1. We claim that $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime number. To check whether $\mathbb{Z}/n\mathbb{Z}$ is a field, we only have to find out if every nonzero element has a muliplicative inverse. Let us look at some examples first:

For $n = 2$, the tables defining addition and multiplication look as follows:

$$\begin{array}{ccccc} + & \vdots & \bar{0} & \bar{1} \\ \cdots & \cdot & \cdots & \cdots \\ \bar{0} & \vdots & \bar{0} & \bar{1} \\ \bar{1} & \vdots & \bar{1} & \bar{0} \end{array}$$

$$\begin{array}{ccccc} \bullet & \vdots & \bar{1} \\ \cdots & \cdot & \cdots \\ \bar{1} & \vdots & \bar{1} \end{array}$$

Since $\bar{1} \cdot \bar{1} = \bar{1}$, $\mathbb{Z}/2\mathbb{Z}$ is a field, denoted by $\mathbb{F}_2$.

For $n = 3$, the tables defining addition and multiplication look as follows:

$+$	$\vdots$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\dots$	$\cdot$	$\dots$	$\dots$	$\dots$
$\bar{0}$	$\vdots$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\vdots$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\vdots$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\bullet$	$\vdots$	$\bar{1}$	$\bar{2}$
$\dots$	$\cdot$	$\dots$	$\dots$
$\bar{1}$	$\vdots$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\vdots$	$\bar{2}$	$\bar{1}$

Again, every nonzero element has an inverse (note that $\bar{2}^{-1} = \bar{2}$), and therefore $\mathbb{Z}/3\mathbb{Z}$ is a field, denoted by $\mathbb{F}_3$.

Here are the tables for $n = 4$:

$+$	$\vdots$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\dots$	$\cdot$	$\dots$	$\dots$	$\dots$	$\dots$
$\bar{0}$	$\vdots$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\vdots$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\vdots$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\vdots$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\bullet$	$\vdots$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\dots$	$\cdot$	$\dots$	$\dots$	$\dots$
$\bar{1}$	$\vdots$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\vdots$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\vdots$	$\bar{3}$	$\bar{2}$	$\bar{1}$

The elements $\bar{1}$ and $\bar{3}$ have inverses with respect to multiplication, but $\bar{2}$ has no inverse. Therefore, $\mathbb{Z}/4\mathbb{Z}$ is *not* a field.

PROPOSITION 1.8. *The set $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime number.*

PROOF. Let us first assume that n is not a prime number. Then n can be factored as $n = n_1 n_2$ with $1 < n_1 < n, 1 < n_2 < n$. In $\mathbb{Z}/n\mathbb{Z}$, we obtain

$$\overline{n_1} \neq \bar{0}, \quad \overline{n_2} \neq \bar{0}, \quad \text{but} \quad \overline{n_1} \cdot \overline{n_2} = \overline{n} = \bar{0}.$$

Therefore, neither $\overline{n_1}$ nor $\overline{n_2}$ are invertible, and $\mathbb{Z}/n\mathbb{Z}$ is not a field.

Let us assume now that n is a prime number. We have to show that every nonzero element $\overline{m}$ in $\mathbb{Z}/n\mathbb{Z}$ has an inverse with respect to multiplication. We first note that

$$\overline{m}\,\overline{i} = \bar{0}$$

is equivalent to the fact that n divides $m\,i$. But n is a prime number and m is not divisible by n, so i must be divisible by n, which means that $\overline{i} = \overline{0}$. This implies that

$$\overline{m}\,\overline{k} = \overline{m}\,\overline{j} \Longleftrightarrow \overline{k} = \overline{j},$$

just take $i = k - j$. If we now let $\overline{k}$ run through the non-zero elements

$$\{\overline{1}, \overline{2}, \ldots, \overline{n-1}\}$$

of $\mathbb{Z}/n\mathbb{Z}$, then the $n-1$ elements $\overline{m}\,\overline{k}$ are all distinct, and hence one of them has to equal $\overline{1}$, which had to be shown. □

REMARKS 1.9. 1. Prime numbers are usually denoted by the letter p, and the corresponding field $\mathbb{Z}/p\mathbb{Z}$ with p elements is denoted by $\mathbb{F}_p$. In our applications to coding theory, we will be dealing with $\mathbb{F}_2$, the field with 2 elements.

2. The fields $\mathbb{F}_p$ are examples of **finite fields**, i.e., fields with only finitely many elements. One can show that the number of elements in any finite field has to be a power of a prime number p.

2. Mathematical Induction

We will frequently use the principle of mathematical induction. Let $\mathbb{N}$ denote the set of all natural numbers, i.e., the set of positive integers.

THEOREM 1.10 (The Principle of Mathematical Induction). *Let $P(n)$ be a statement depending on the number n. Assume that $P(1)$ is true and the truth of the implication*

$$P(k) \text{ is true} \Longrightarrow P(k+1) \text{ is true.}$$

Then $P(n)$ is true for all $n \in \mathbb{N}$.

Although this is very plausible, it is in fact an axiom about the natural numbers, equivalent to the axiom that every nonempty subset of $\mathbb{N}$ contains a smallest element.

REMARK 1.11. Sometimes it is more suitable to replace the condition

$$P(k) \text{ is true} \Longrightarrow P(k+1) \text{ is true}$$

by the condition

$$P(i) \text{ is true for all } i \leq k \Longrightarrow P(k+1) \text{ is true,}$$

which leads to an equivalent formulation of the principle of mathematical induction.

Let us consider a few examples:

EXAMPLES 1.12. a. Prove that $n! \geq 2^{n-1}$ for all $n \in \mathbb{N}$.

For $n = 1$, we have $1! = 1 = 2^0 = 1$, so the **base case** $P(1)$ is true. We now make the **inductive hypothesis** by assuming that $P(k)$ is true, i.e., that $k! \geq 2^{k-1}$. We have

$$(k+1)! = (k+1)\,k! \geq (k+1)\,2^{k-1} \geq 2 \cdot 2^{k-1} = 2^k.$$

Therefore, $P(k+1)$ is true, and by the principle of induction, we have $P(n)$ true for all $n \in \mathbb{N}$.

b. Show that, for any real number $x \neq 1$ and any $n \geq 1$,

$$1 + x + x^2 + \cdots + x^{n-1} = \frac{1 - x^n}{1 - x}.$$

For $n = 1$, both sides are equal to 1, so $P(1)$ is true. Let us assume now that $P(k)$ is true, i.e.,

$$1 + x + x^2 + \cdots + x^{k-1} = \frac{1 - x^k}{1 - x}.$$

Then

$$1 + x + x^2 + \cdots + x^k = \frac{1 - x^k}{1 - x} + x^k = \frac{1 - x^k + x^k(1 - x)}{1 - x} = \frac{1 - x^{k+1}}{1 - x}.$$

c. Show that every natural number > 1 contains a prime factor.

Here, the base case is $n = 2$, which is a prime number. We assume now that all integers i with $2 \leq i \leq k-1$ contain a prime factor, and have to show that k contains a prime factor. If k itself is a prime number, then we are done. Otherwise, k can be factored as $k = l \cdot m$ with $l, m \geq 2$. Then $2 \leq l \leq k - 1$, and by the inductive hypothesis l contains a prime factor, so k contains the same prime factor.

3. Polynomial Rings

Throughout this section, we fix a field F. We let x denote an indeterminate and consider the set $F[x]$ of all polynomials $f(x)$, i.e., of finite formal sums

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

where $n \geq 0$ and the coefficients a_i are elements of the field F. If $a_n \neq 0$, then $f(x)$ has **degree** n, written as

$$\deg f(x) = n.$$

The zero polynomial 0 does *not* have a degree. Note that the polynomials of degree 0 are precisely the nonzero elements in F.

Two nonzero polynomials

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

and

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m$$

are equal if and only if they have the same degree and coefficients, i.e., $m = n$ and $a_0 = b_0$, $a_1 = b_1, \ldots$.

Addition and multiplication of polynomials are defined as usual.

Example 1.13. Let

$$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3$$

and

$$g(x) = b_0 + b_1 x + b_2 x^2.$$

Then

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + a_3 x^3,$$

and

$$f(x)g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x +$$

$$+(a_1b_1 + a_0b_2 + a_2b_0)x^2 + (a_1b_2 + a_2b_1 + a_3b_0)x^3 + (a_2b_2 + a_3b_1)x^4 + a_3b_2x^5.$$

With respect to addition, $F[x]$ is an abelian group. Furthermore, multiplication is associative,

$$1 \cdot f(x) = f(x) \cdot 1 = f(x)$$

for all $f(x) \in F[x]$, and the distributivity law holds. Sets R with two operations $+$ and $\cdot$ having these properties are called **rings**. If multiplication is commutative, as it is with $F[x]$, then R is called a **commutative ring**.

EXAMPLES 1.14. a. The ring of integers $\mathbb{Z}$ is a commutative ring.

b. Every field F is a commutative ring.

c. For any $n > 1$, the set $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring.

d. For any field F and any $n \geq 2$, the set $M_n(F)$ of all $n \times n$-matrices with coefficients in F is a non-commutative ring.

DEFINITION 1.15. We call $F[x]$ the **polynomial ring with coefficients in** F. We sometimes simply write f instead of $f(x)$.

The following lemma is obvious from the definitions of addition and multiplication in $F[x]$.

LEMMA 1.16. *For any two nonzero polynomials $f, g \in F[x]$, we have*

$$\deg(f + g) \leq \max\{\deg f, \deg g\}$$

and

$$\deg fg = \deg f + \deg g.$$

Here are some consequences:

COROLLARY 1.17. *a. If $fg = 0$, then either $f = 0$ or $g = 0$.*

b. If $fg = hg$ and $g \neq 0$, then $f = h$ (cancellation).

PROOF. a. If both $f \neq 0$ and $g \neq 0$, then the coefficient of $x^{\deg f + \deg g}$ in fg is nonzero as the product of the nonzero coefficients of $x^{\deg f}$ in f and $x^{\deg g}$ in g. Hence $fg \neq 0$.

b. We have $(f - h)g = 0$ and $g \neq 0$, so $f - h = 0$ by i.

□

The following result shows in particular that $F[x]$ can never be a field.

COROLLARY 1.18. *Let f be a nonzero polynomial. Then there exists a polynomial g for which $fg = 1$ if and only if* $\deg f = 0$.

PROOF. Let us assume first that $\deg f = 0$. Then $f(x) = a \in F$, $a \neq 0$, and we can take $g(x) = a^{-1}$. If, on the other hand, $fg = 1$, then, by Lemma 1.16,

$$\deg f + \deg g = \deg fg = \deg 1 = 0,$$

which shows that $\deg f = 0$. □

The polynomial ring $F[x]$ has properties very similar to those of the ring of integers $\mathbb{Z}$. In particular, there is also a division algorithm.

THEOREM 1.19 (Division Algorithm). *Let $f, g \in F[x]$ with $g \neq 0$. There exist uniquely determined polynomials q and r such that*

$$f = qg + r$$

and either $r = 0$ or $\deg r < \deg g$.

PROOF. We first show the existence of q and r. Let

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k$$

and

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m$$

with $a_k \neq 0$ and $b_m \neq 0$, so

$$\deg f = k, \quad \deg g = m.$$

If $m = 0$, so $g(x) = b_0$ is a nonzero element in F, then

$$f(x) = (f(x)b_0^{-1})g(x).$$

Hence, $q(x) = f(x)b_0^{-1}$ and $r = 0$.

Assume now that $\deg g = m > 0$. We will prove the result by induction on the degree of f. If $\deg f < \deg g$, then

$$f = 0 \cdot g + f$$

is of the desired form with $q = 0$ and $r = f$. In particular, the result is true for $\deg f = 0$. Let assume now that the result is true for all polynomials of degree $\leq k - 1$, and let f as above be of degree $k \geq m$. Put

$$f_1(x) = f(x) - a_k b_m^{-1} x^{k-m} g(x).$$

Then $f_1(x)$ is of degree $\leq k - 1$, and by the induction hypothesis we have

$$f_1 = q_1 g + r_1$$

with $r = 0$ or $\deg r_1 < \deg g = m$. We obtain

$$f = f_1 + a_k b_m^{-1} x^{k-m} g = q_1 g + r_1 + a_k b_m^{-1} x^{k-m} g = (q_1 + a_k b_m^{-1} x^{k-m}) g + r_1,$$

and, therefore, the result with $q = q_1 + a_k b_m^{-1} x^{k-m}$ and $r = r_1$.

To show uniqueness, let us assume that

$$f = qg + r = q'g + r'$$

with $r = 0$ or $\deg r < \deg g$ and $r' = 0$ or $\deg r' < \deg g$. Then $r - r' = (q' - q)g$. If $r \neq r'$, then the lefthand side has degree $< \deg g$, whereas the righthand side has degree $\geq \deg g$ by Lemma 1.16. This is a contradiction, so $r = r'$. Therefore

$$(q' - q)g = 0.$$

Since $g \neq 0$, Corollary 1.18 shows that $q' = q$, which proves uniqueness. □

Let us compute an example.

EXAMPLE 1.20. Let

$$f(x) = 3x^3 + x^2 - x + 1, \quad g(x) = x^2 + 2x - 1 \in \mathbb{Q}[x].$$

Then

$$f_1(x) = f(x) - 3xg(x) = -5x^2 + 2x + 1.$$

We repeat the argument:

$$f_2(x) = f_1(x) + 5g(x) = 12x - 4.$$

Hence,

$$f(x) = f_1(x) + 3xg(x) = f_2(x) - 5g(x) + 3xg(x) = (3x - 5)g(x) + (12x - 4).$$

Here

$$q(x) = 3x - 5 \quad \text{and} \quad r(x) = 12x - 4.$$

The following results, with only minor changes, hold equally well for the ring of integers $\mathbb{Z}$.

DEFINITION 1.21. Given two polynomials f and g in $F[x]$, we say that f **divides** g (written as $f \mid g$) if $g = f \cdot h$ for some polynomial $h \in F[x]$. The polynomial g is then a **multiple** of f. A polynomial p of degree ≥ 1 is **prime**, or **irreducible**, if it is only divisible by polynomials of degree 0 and any product of itself with a polynomial of degree 0. In other words, a polynomial $p(x)$ is irreducible if

$$p = f \cdot g \implies \deg f = 0 \quad \text{or} \quad \deg g = 0.$$

In particular, all polynomials of degree 1 are irreducible.

Given polynomials $g_1, \ldots, g_k$, we say that $d \in F[x]$ is a **greatest common divisor** (**GCD** for short) of $g_1, \ldots, g_k$ if d is a common divisor of $g_1, \ldots, g_k$, i.e., if

$$d \mid g_1, \quad d \mid g_2, \ldots, d \mid g_k,$$

and if any other common divisor d' of $g_1, \ldots, g_k$ divides d.

PROPOSITION 1.22. *Let $g_1, \ldots, g_k$ be arbitrary nonzero polynomials in $F[x]$.*

i. There exists a greatest common divisor d of $g_1, \ldots, g_k$.

ii. If d and d' are greatest common divisors of $g_1, \ldots, g_k$, then $d' = a \cdot d$ for some $a \in F$, $a \neq 0$.

iii. If d is a greatest common divisor of $g_1, \ldots, g_k$, then there are polynomials $f_1, \ldots, f_k$ in $F[x]$ such that

$$d = f_1 g_1 + f_2 g_2 + \cdots + f_k g_k.$$

PROOF. Consider the set S of all polynomials of the form

$$f_1 g_1 + f_2 g_2 + \cdots + f_k g_k,$$

where $f_1, \ldots, f_k$ are arbitrary polynomials in $F[x]$. Clearly, S contains $g_1, \ldots, g_k$. In particular, S is nonempty. Furthermore, it is closed under addition and under multiplication by arbitrary polynomials, i.e., if $f \in S$, then $q \cdot f \in S$ for all $q \in F[x]$.

Let d be a nonzero polynomial in S of smallest degree. We claim that d is a greatest common divisor of $g_1, \ldots, g_k$. Let us show first that $d \mid g_i$ for $1 \leq i \leq k$. By the Division Algorithm, we find q_i and r_i such that

$$g_i = q_i d + r_i$$

with $r_i = 0$ or $\deg r_i < \deg d$. Now

$$r_i = g_i - q_i d \in S,$$

and since d was chosen to have smallest degree, we must have $r_i = 0$. Therefore, d is a common divisor of $g_1, \ldots, g_k$.

Assume now that d' is another common divisor of $g_1, \ldots, g_k$. Then clearly d' divides any polynomial in S. In particular, d' divides d. This proves parts i and iii.

If d and d' are both greatest common divisors of $g_1, \ldots, g_k$, then

$$d \mid d' \quad \text{and} \quad d' \mid d.$$

This implies that $\deg d = \deg d'$, and therefore Lemma 1.16 implies that

$$d' = a \cdot d$$

with $\deg a = 0$, so $a \in F$, $a \neq 0$. □

Since greatest common divisors differ only by nonzero constants, we can normalize the highest nonzero coefficient to be 1. Polynomials of this form are called **monic**. There is then a *unique* monic greatest common divisor for any given polynomials $g_1, \ldots, g_k$.

Important consequences include the following:

COROLLARY 1.23. *Polynomials $g_1, \ldots, g_k \in F[x]$ are relatively prime (i.e., their GCD equals 1) if and only if there exist polynomials $f_1, \ldots, f_k \in F[x]$ such that*

$$f_1 g_1 + f_2 g_2 + \cdots + f_k g_k = 1.$$

COROLLARY 1.24. *Assume that p is irreducible. If $p \mid fg$, then*

$$p \mid f \quad \textit{or} \quad p \mid g.$$

PROOF. Suppose that $p \nmid f$. Then p and f are relatively prime, and therefore, by Proposition 1.22,

$$h_1 p + h_2 f = 1$$

for some polynomials h_1, h_2. Mulitplying by g, we obtain

$$h_1 pg + h_2 fg = g.$$

The lefthand side is divisible by p, and hence the same is true for the righthand side. □

If a polynomial $f(x)$ of degree ≥ 1 is not irreducible, then it factors as

$$f = g \cdot h$$

with $\deg g \geq 1$ and $\deg h \geq 1$. Since

$$\deg f = \deg g + \deg h,$$

we see that $\deg g < \deg f$ and $\deg h < \deg f$. Using induction on the degree, we see that every polynomial f of degree ≥ 1 can be written as a product of irreducible

polynomials, the same way a positive integer ≥ 2 can be written as a product of prime numbers. The prime numbers occurring are uniquely determined, and the following result shows that this is also true for polynomials:

THEOREM 1.25 (Unique Factorization). *Every polynomial $f(x) \in F[x]$ of degree ≥ 1 can be written as a product of irreducible polynomials:*

$$f = p_1 \cdot p_2 \cdots p_r.$$

Moreover if

$$f = q_1 \cdot q_2 \cdots q_s$$

is another presentation of f as a product of irreducible polynomials $q_1, \ldots, q_s$, then $r = s$, and, after renumbering the q_i's if necessary, we have

$$q_i = a_i \cdot p_i \quad \text{for } i = 1, \ldots, r,$$

where $\deg a_i = 0$.

PROOF. As mentioned above, we can proceed by induction on the degree to show that f factors into a product of irreducible polynomials. To prove uniqueness, let us assume that we have two factorizations

$$f = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s$$

into a product of irreducible polynomials with $r \leq s$. We use induction on r. If $r = 1$, then f is irreducible, and the result is clear. Let us assume now that the result is true whenever f factors into a product of $< r$ irreducible polynomials, and let us look at the two factorizations given above. Since p_1 divides f, it divides the product $q_1 \cdot q_2 \cdots q_s$. By Corollary 1.24, p_1 then divides one of the factors q_j. Renumbering the q_j's if necessary, we may assume that $p_1 \mid q_1$. But q_1 is irreducible as well, so

$$q_1 = a_1 \cdot p_1$$

for some a_1 of degree 0. We can now cancel by Corollary 1.18 and obtain

$$p_2 \cdots p_r = a_1 q_2 \cdots q_s = q_2' \cdots q_s,$$

where $q_2' = a_2 q_2$ is again irreducible. The induction hypothesis now gives the result. □

If p and q are irreducible factors of a polynomial f, then they are either relatively prime or they differ by a factor of degree 0, i.e., we can have $q = c \cdot p$ for some $c \in F$, $c \neq 0$. In this case f would be divisible by p^2. If we combine in this way all the irreducible factors, which are not relatively prime to each other, then we obtain:

COROLLARY 1.26. *Every polynomial $f \in F[x]$ can be written as*

$$f = a \cdot p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

with $a \in F$, $a \neq 0$ and the p_i's irreducible and pairwise relatively prime, i.e., any two of them are relatively prime.

In calculus, we view polynomials as maps from $\mathbb{R}$ to $\mathbb{R}$ by inserting real numbers for x. We can do this over arbitrary fields F.

DEFINITION 1.27. If $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_kx^k$ is a polynomial in $F[x]$ and $c \in F$, then we call

$$f(c) = a_0 + a_1c + a_2c^2 + \cdots + a_kc^k$$

the **value of** f **at** c. We call c a **zero** or **root** of f if $f(c) = 0$. Given f, we obtain the corresponding **polynomial function** from F to F by

$$c \mapsto f(c).$$

Over $\mathbb{R}$, two polynomial functions are the same if and only if the polynomials are the same since

$$f(c) = g(c) \text{ for all } c \in \mathbb{R} \quad \Longrightarrow \quad f = g.$$

The same statement is not true for finite fields:

EXAMPLE 1.28. Let $f(x) = x^2 + x$ and let $F = \mathbb{F}_2$. The values of f at 0 or 1 are both 0 so that, as a polynomial function, f is the zero function, but of course f is not the zero polynomial.

We leave it as an exercise to show that, for two polynomials f and g and all $c \in F$,

$$(f + g)(c) = f(c) + g(c) \quad \text{and} \quad (fg)(c) = f(c)g(c).$$

PROPOSITION 1.29. *Let $f \in F[x]$ be a polynomial and $c \in F$. Then*

$$c \text{ is a root of } f \quad \Longleftrightarrow \quad (x - c) \mid f.$$

PROOF. We can divide f by $x - c$,

$$f = q(x - c) + r,$$

with a remainder r that is either 0 or of degree $< \deg(x-c) = 1$, so $r \in F$. Evaluating f at c gives

$$f(c) = (c - c) + r = r,$$

so that we can write

$$f = q(x - c) + f(c).$$

The result is now obvious. □

Here is an easy consequence.

COROLLARY 1.30. *Let $f \in F[x]$ be a polynomial of degree n. Then:*

a. f has at most n roots in F.

b. if f has precisely n roots, it splits completely into linear factors, i.e., is of the form

$$f = a(x - c_1) \cdots (x - c_n)$$

with $a, c_1, \ldots, c_n \in F$.

Over an arbitrary field F, there will usually be lots of polynomials without any roots. For example,

$$x^2 - 2 \in \mathbb{Q}[x]$$

does not have a root, as $\sqrt{2}$ is not a rational number. The same polynomial, however, viewed as a polynomial in $\mathbb{R}[x]$, has the two roots $\pm\sqrt{2}$. The polynomial

$$x^2 + 1 \in \mathbb{R}[x]$$

has no roots, but as a polynomial in $\mathbb{F}_2[x]$ it has two: $\bar{1}$ twice. As we shall now discuss, there is a field $\mathbb{C}$ called the complex numbers such that every polynomial in $\mathbb{C}[X]$ has a root in $\mathbb{C}$ and therefore splits completely into linear factors.

The easiest way to define $\mathbb{C}$ is to start with a 2-dimensional vector space over $\mathbb{R}$ with basis 1 and i. Every complex number z can then be written uniquely as

$$z = a + bi$$

with $a, b \in \mathbb{R}$. Addition is the usual vector space addition:

$$(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i.$$

In this way, we obtain an abelian group under " $+$ ". Multiplication is now defined in such a way that $i^2 = -1$:

$$(a_1 + b_1 i) \cdot (a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i.$$

One can easily check associativity, distributivity, and of course that $1 \cdot z = z$ for all z. To show that $\mathbb{C}$ is a field, we need to show that every non-zero z has an inverse with respect to multiplication. Let us first introduce the **complex conjugate** $\overline{z}$ of a complex number z. If $z = a + bi$, then $\overline{z} = a - bi$. Then

$$z\overline{z} = a^2 + b^2,$$

which is equal to 0 if and only if $z = 0$. For $z = a + bi \neq 0$, we obtain

$$z^{-1} = \frac{1}{z\overline{z}} \cdot \overline{z} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i.$$

To summarize, we have shown:

PROPOSITION 1.31. *The set of complex numbers $\mathbb{C}$ is a field.*

We define the **absolute value** $|z|$ of the complex number $z = a + bi$ to be $\sqrt{a^2 + b^2}$. Therefore, we have

$$z\overline{z} = |z|^2.$$

It is sometimes easier to consider vector spaces over $\mathbb{C}$, as opposed to $\mathbb{R}$. The primary reason for this lies in the following theorem, which we quote without proof.

THEOREM 1.32 (Fundamental Theorem of Algebra). *Every polynomial in $\mathbb{C}[x]$ of degree ≥ 1 has a root.*

Let $f \in \mathbb{C}[x]$ be an arbitrary polynomial of degree ≥ 1. Then f has a root c in $\mathbb{C}$ by the Fundamental Theorem. By Proposition 1.29, this is equivalent to the fact that f is divisible by $x - c$. If $\deg f \geq 2$, then this implies that f is *not* irreducible. Therefore, the irreducible polynomials in $\mathbb{C}[x]$ are precisely the linear polynomials. By Corollary 1.30, we obtain:

COROLLARY 1.33. *Every polynomial $f \in \mathbb{C}[x]$ of degree $n \geq 1$ can be written as a product*

$$f(x) = a(x - c_1)^{e_1}(x - c_2)^{e_2} \cdots (x - c_r)^{e_r},$$

where $a \in \mathbb{C}$, $a \neq 0$, $c_1, \ldots, c_r$ are the distinct roots of f in $\mathbb{C}$, and $e_1, \ldots, e_r$ are positive integers.

CHAPTER 2

VECTOR SPACES

In this chapter, we recall the basic features of vector spaces, allowing scalars from an arbitrary field F.

DEFINITION 2.1. Let F be a field. An **F-vector space**, or **vector space over F**, is a nonempty set V with elements called **vectors** and two compositions, addition "+" of vectors and multiplication of vectors by elements of F, called **scalars**, for which the following properties hold:

1. V is an abelian group under addition.
2. $a(v+w) = av + aw$ for all $a \in F$, $v, w \in V$.
3. $(a+b)v = av + bv$ for all $a, b \in F$, $v \in V$.
4. $(ab)v = a(bv)$ for all $a, b \in F$, $v \in V$.
5. $1\,v = v$ for all $v \in V$.

Let us consider some examples:

EXAMPLES 2.2. a. Let F^n denote the set of all n-tuples $(a_1, a_2, \ldots, a_n)$ with $a_i \in F$, $1 \leq i \leq n$. This is an F-vector space, with addition and scalar multiplication being defined componentwise. The space F^n is the natural generalization of $\mathbb{R}^n$ to arbitrary fields.

b. The set $M_{mn}(F)$ of all $m \times n$-matrices with entries in F is an F-vector space under matrix addition and scalar multiplication.

c. The polynomial ring $F[x]$ is an F-vector space. Sometimes, if $F[x]$ is considered as a vector space rather than as a ring, it is denoted by $P(F)$. In the same manner, we can consider the set of all polynomials from $F[x]$ of degree $\leq n$. This F-vector space is denoted by $P_n(F)$.

d. Let $\mathcal{F}(F)$ denote the set of all functions $f : F \to F$. For $f, g \in \mathcal{F}(F)$, define a function $f + g$ by

$$(f+g)(a) = f(a) + g(a),$$

and define scalar multiplication of a function f by a scalar $b \in F$ by

$$(bf)(a) = bf(a).$$

It is easily checked that all the axioms of an F-vector space are satisfied.

REMARK 2.3. We note that the following properties hold in an F-vector space V. The proofs are identical to the proofs of Lemma 1.6 for fields:

1. $0\,v = 0$ for all $v \in V$. (Note: The 0 on the lefthand side is the 0 in F. The 0 on the righthand side is the zero vector in V.)

2. $-v = (-1)v$ for all $v \in V$.

DEFINITION 2.4. A nonempty subset W of an F-vector space V is a **subspace** of V if W, equipped with vector addition and scalar multiplication as a subset of V, is itself an F-vector space.

We note that, in particular, the sum $v + w$ of two vectors $v, w \in W$ has to lie in the subspace W and that any scalar multiple av of a vector $v \in W$ has to lie in W. In other words, W has to be *closed under addition and scalar multiplication*. The following result shows that these two conditions suffice to determine whether a subset is a subspace or not.

LEMMA 2.5. *A nonempty subset W of an F-vector space V is a subspace of V if and only if W is closed under addition and scalar multiplication.*

PROOF. We saw already that these conditions are necessary. Let us assume now that W is closed under addition and scalar multiplication. It is clear that the properties 2–5 in the definition of an F-vector space hold for vectors in W, since they hold in V. Furthermore, addition is associative since this is true in V. It remains to show that the zero vector lies in W and that $v \in W$ implies $-v \in W$, so that W is a group with respect to addition.

Since W is nonempty, there is some vector $v \in W$. Now $-v = (-1)v$ by Remark 2.3. Hence $-v \in W$, since W is closed under scalar multiplication. Since W is closed under addition, we obtain $v + (-v) = 0 \in W$, as claimed. □

EXAMPLES 2.6. a. In F^n, consider the subset W of all vectors v such that $Av = 0$, where A is a given $m \times n$-matrix. We call W the **nullspace** of A.

b. In $M_{mn}(F)$, consider the subset of all matrices whose first row is equal to 0.

c. The vector space $P_n(F)$ is a subspace of $P(F)$.

d. In $\mathcal{F}(\mathbb{R})$, consider the subset of all continuous functions.

DEFINITION 2.7. Let V denote a vector space over a field F. Given vectors $v_1, v_2, \ldots, v_n \in V$ and scalars $a_1, a_2, \ldots, a_n \in F$, the finite sum

$$a_1v_1 + a_2v_2 + \cdots + a_nv_n$$

is called a **linear combination** of $v_1, v_2, \ldots, v_n$.

The set $S(v_1, v_2, \ldots, v_n)$ of all possible linear combinations of $v_1, v_2, \ldots, v_n$ is closed under vector addition and scalar multiplication and is therefore a subspace of V, the subspace **generated** or **spanned** by $v_1, v_2, \ldots, v_n$. If $S \subset V$ is any subspace of V and $v_1, v_2, \ldots, v_n$ are in S, then every linear combination of the vectors $v_1, v_2, \ldots, v_n$ lies in S as well. Hence,

$$S(v_1, v_2, \ldots, v_n) \subset S.$$

Therefore, $S(v_1, v_2, \ldots, v_n)$ is the *smallest* subset of V containing $v_1, v_2, \ldots, v_n$.

A subspace S is said to be **finitely generated** if there exist some vectors $v_1, v_2, \ldots, v_n$ so that

$$S = S(v_1, v_2, \ldots, v_n).$$

More generally, we can consider an arbitrary nonempty subset E of vectors from V and define $S(E)$ as the set of all possible linear combinations of vectors from E. Note that each linear combination involves only finitely many vectors, but these vectors may vary. Again, $S(E)$ is a subspace of V; in fact, it is the smallest subspace of V containing E.

For a subspace S generated by a single nonzero vector v, we will often write

$$S(v) = Fv.$$

EXAMPLES 2.8. a. The set $\{1, x, x^2, \ldots, x^n\}$ generates $P_n(F)$, and the set $\{1, x, x^2, \ldots\}$ generates $P(F)$. The latter set is infinite.

b. If A is a matrix in $M_{mn}(F)$, then the **row space** of A is the subspace of F^n generated by the rows of A, and the **column space** of A is the subspace of F^m generated by the columns of A.

DEFINITION 2.9. The vectors $v_1, v_2, \ldots, v_n$ are called **linearly independent** if the only linear combination of $v_1, v_2, \ldots, v_n$ representing the zero vector is the trivial one, hence if

$$a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0 \quad \Longrightarrow \quad a_i = 0 \text{ for all } i = 1, 2, \ldots, n.$$

Vectors which are not linearly independent are called **linearly dependent**. Note that the zero vector 0 is always linearly dependent and that a single nonzero vector is always linearly independent.

PROPOSITION 2.10. *The vectors $v_1, v_2, \ldots, v_n$ are linearly independent if and only if every vector $v \in S(v_1, \ldots, v_n)$ can be written uniquely as a linear combination of $v_1, v_2, \ldots, v_n$.*

PROOF. Assume first that the vectors $v_1, v_2, \ldots, v_n$ are linearly independent, and let $v \in S(v_1, \ldots, v_n)$. Let

$$v = a_1v_1 + a_2v_2 + \cdots + a_nv_n$$

and

$$v = b_1v_1 + b_2v_2 + \cdots + b_nv_n$$

be two presentations of v as a linear combination of $v_1, v_2, \ldots, v_n$. Subtracting the two equations we obtain

$$0 = (a_1 - b_1)v_1 + (a_2 - b_2)v_2 + \cdots + (a_n - b_n)v_n.$$

Since by assumption the vectors $v_1, v_2, \ldots, v_n$ are linearly independent, we obtain

$$a_1 = b_1, a_2 = b_2, \ldots, a_n = b_n,$$

as claimed.

Conversely, if we assume that the presentation of every vector from $S(v_1, \ldots, v_n)$ is unique, then in particular this applies to the zero vector, which is in $S(v_1, \ldots, v_n)$. Therefore,

$$0 = 0 \cdot v_1 + 0 \cdot v_2 + \cdots + 0 \cdot v_n$$

is the only possible linear combination for the zero vector, which means that $v_1, \ldots, v_n$ are linearly independent. □

We can extend the definitions of linear independence and dependence to arbitrary subsets E of V. That is, E will be a **linearly independent set** if any finite number of vectors from E are linearly independent and will be a **linearly dependent set** otherwise.

DEFINITION 2.11. Let S be a subspace of V. A set B of vectors in S is a **basis** of S if B is a linearly independent set which generates S. If $S = \{0\}$ is the subspace consisting only of the zero vector, then 0 is considered to be a basis vector.

EXAMPLES 2.12. a. In F^n, we have the **standard basis** $e_1, e_2, \ldots, e_n$, where

$$e_i = (0, \ldots, 0, \underset{i}{1}, 0, \ldots, 0),$$

the 1 being in the ith position.

b. In $M_{mn}(F)$, we have a basis consisting of matrices e_{ij}, $1 \leq i \leq m, 1 \leq j \leq n$, which have a 1 in the ij-th position and 0's everywhere else.

c. In $P_n(F)$, we have the basis $B = \{1, x, x^2, \ldots, x^n\}$. In $P(F)$, we have the basis $B = \{1, x, x^2, \ldots, x^n, \ldots\}$ consisting of *all* the powers of x.

The main results about finitely generated vector spaces are summarized in the following two theorems and their consequences.

THEOREM 2.13. *Let E be a finite set of vectors in V, and let $E_0 \subset E$ be a linearly independent subset. Then there exists a basis B of the subspace $S(E)$ such that*

$$E_0 \subset B \subset E.$$

In other words, the linearly independent subset E_0 can be extended to a basis B of $S(E)$ by adding suitable vectors from E to E_0.

PROOF. If $S(E_0) = S(E)$, then E_0 is a basis of $S(E)$, and we are done. Let us assume then that $S(E_0) \neq S(E)$. Let $E_0 = \{v_1, v_2, \ldots, v_m\}$. Our assumption implies that there is at least one vector $v \in E$ which is not contained in $S(E_0)$. We now define $E_1 = E_0 \cup \{v\} = \{v_1, \ldots, v_m, v\}$.

Claim: E_1 is linearly independent. To show this, let us assume that

$$a_1 v_1 + a_2 v_2 + \cdots + a_m v_m + av = 0.$$

Then $a = 0$, since otherwise

$$v = -\frac{1}{a}(a_1 v_1 + \cdots + a_m v_m)$$

would be a linear combination of $v_1, \ldots, v_m$, hence in $S(E_0)$, contradicting our assumption. However, if $a = 0$, then the linear combination reads $a_1 v_1 + \cdots + a_m v_m = 0$, and the linear independence of $v_1, \ldots, v_m$ implies that $a_1 = 0, \ldots, a_m = 0$ as well.

We can now apply the same arguments to the independent set E_1. Either $S(E_1) = S(E)$, in which case we are done, or we can enlarge E_1 to a linearly independent subset E_2 of E by adding a vector from E to E_1, etc. Since E is a finite set, this procedure has to stop, and we end up with a basis B of $S(E)$ that contains E_0 and lies in E. □

Theorem 2.13 has some obvious important consequences:

COROLLARY 2.14. *Let V be a finitely generated F-vector space. Then*

a. V has a finite basis.

b. Any basis of a subspace of V can be extended to a basis of V.

c. Any finite set of generators of V contains a basis.

EXAMPLE 2.15. Consider

$$E = \{(1,1,1),(0,1,1),(1,0,0),(1,0,1)\}$$

as a subset of $\mathbb{R}^3$, and take $E_0 = \{(1,1,1)\}$. Clearly $(0,1,1)$ is not contained in $S(E_0)$. Hence, we can add $(0,1,1)$ to E_0 to obtain a linearly independent set $E_1 = \{(1,1,1),(0,1,1)\}$. The vector $(1,0,0)$ is contained in $S(E_1)$, but $(1,0,1)$ is not. Therefore, we can enlarge E_1 to an independent set E_2 by adding $(1,0,1)$ to E_1:

$$E_2 = \{(1,1,1),(0,1,1),(1,0,1)\}.$$

Clearly, $S(E_2) = S(E)$, and therefore $B = E_2$ is a basis for $S(E)$.

REMARK 2.16. In the special case that $V = F^n$, we can always proceed as follows to find the basis B. Let $E_0 = \{v_1, \ldots, v_k\}$ be a linearly independent set contained in E. Let $v_{k+1}, \ldots, v_r$ denote the vectors in E that are not contained in E_0. We then form the $n \times k$-matrix A that has the vectors v_i as its columns. Then the span $S(E)$ of E is just the column space of A. We recall that elementary row operations on the matrix A do not change linear independence or linear dependence relations of the columns. We reduce A to a row echelon form R. A basis for the column space of R is provided by the columns of R that contain a leading 1, i.e., a 1 that is the first nonzero entry in its row. Therefore, a basis of $S(E)$ is provided by those columns of A that are in the same positions as the leading 1's of R. Since the first m columns of A are linearly independent, the same is true for the first m columns of R. That is, E_0 is part of the basis.

In Example 2.15, the matrix A for the ordered set E, i.e., with the vectors are taken in the order listed, looks like

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}.$$

A row echelon form R for A equals

$$R = \begin{bmatrix} \mathbf{1} & 0 & 1 & 1 \\ 0 & \mathbf{1} & -1 & -1 \\ 0 & 0 & 0 & \mathbf{1} \end{bmatrix}.$$

The leading 1's are in columns 1, 2, and 4. Therefore, we obtain the same result as above.

THEOREM 2.17 (Steinitz' Replacement Theorem). *Let V be a finitely generated F-vector space with a basis*

$$B = \{v_1, v_2, \ldots, v_n\},$$

and let

$$E = \{w_1, w_2, \ldots, w_m\}$$

be an arbitrary linearly independent subset of V. Then $m \leq n$, and E can be extended to a basis of V by adding $n - m$ suitable vectors from B.

PROOF. We try to change the basis B by replacing certain vectors in B with vectors from E. Since B is a basis, we can write

$$(*) \qquad w_1 = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n,$$

where the coefficients a_i are uniquely determined. Since $w_1 \neq 0$, some coefficient a_i is nonzero. If necessary, we can reindex the basis vectors $v_1, v_2, \ldots, v_n$, so that we may assume that $a_1 \neq 0$. Then

$$v_1 = \frac{1}{a_1}(w_1 - a_2 v_2 - \cdots - a_n v_n),$$

which shows that

$$B_1 = \{w_1, v_2, \ldots, v_n\}$$

generates V. We want to show that $w_1, v_2, \ldots, v_n$ are linearly independent, and therefore B_1 is again a basis of V. To do this, assume that

$$b_1 w_1 + b_2 v_2 + \cdots + b_n v_n = 0.$$

If $b_1 \neq 0$, then

$$(**) \qquad w_1 = -\frac{1}{b_1}(b_2 v_2 + \cdots + b_n v_n).$$

Since $a_1 \neq 0$, $(*)$ and $(**)$ are two different linear combinations representing w_1, which contradicts the fact that B is a basis. The assumption $b_1 \neq 0$ was therefore wrong, so $b_1 = 0$. The linear independence of the vectors $v_2, \ldots, v_n$ then implies that the remaining coefficients $b_2, \ldots, b_n$ are equal to 0 as well, which proves linear independence and hence that B_1 is a basis of V.

Let us now assume that we have constructed a basis

$$B_k = \{w_1, w_2, \ldots, w_k, v'_{k+1}, \ldots, v'_n\}$$

of V, where $v'_{k+1}, \ldots, v'_n$ are suitably chosen vectors from B. If $k = m$, then we are done. Assume then that $m > k$. As before, we can write

$$w_{k+1} = a_1 w_1 + a_2 w_2 + \cdots a_k w_k + a_{k+1} v'_{k+1} + \cdots + a_n v'_n$$

in a unique way. Since the vectors $w_1, \ldots, w_{k+1}$ are linearly independent, for some $i \geq k+1$ the coefficient a_i must be nonzero, and we may assume that $i = k+1$, i.e., that $a_{k+1} \neq 0$. As above, this implies that the vectors $w_1, w_2, \ldots, w_{k+1}, v'_{k+2}, \ldots, v'_n$ generate V and form in fact a basis B_{k+1} of V.

Continuing in this way, we construct bases B_i of V for $i = 1, 2, \ldots, m$, provided that $m \leq n$. Then B_m is then the basis we are looking for. Assume finally that $m > n$. Then $B_n = \{w_1, \ldots, w_n\}$ is a basis for V. In particular, w_{n+1} would be a linear combination of $w_1, \ldots, w_n$, contradicting the linear independence of E. Therefore, $m \leq n$. □

As an immediate consequence, we obtain:

COROLLARY 2.18. *Any two bases of a finitely generated vector space contain the same number of elements.*

DEFINITION 2.19. The number of elements in any basis of a finitely generated vector space V is called the **dimension** of V and denoted by $\dim V$. By definition, the dimension of the 0-vector space is equal to 0. In place of finitely generated, we often use the terminology **finite dimensional**.

EXAMPLES 2.20. a. $\dim F^n = n$.

b. $\dim P_n(F) = n + 1$.

c. $\dim M_{mn}(F) = mn$.

COROLLARY 2.21. *Every subspace S of a finite-dimensional F-vector space V is finite-dimensional, and* $\dim S \leq \dim V$.

PROOF. Clearly, the result is true if $S = (0)$. Hence, we may assume that S contains a nonzero vector v_1. Let $E_1 = \{v_1\}$. If $S(E_1) = S$, then we are done. If not, then we can find a vector $v_2 \in S$ such that $E_2 = \{v_1, v_2\}$ is linearly independent. We can continue as in the proof of Theorem 2.13 and construct linearly independent sets $E_k = \{v_1, \ldots, v_k\} \subset S$ for $k = 1, 2, \ldots$. This process has to terminate since the possible number of linearly independent vectors is bounded by $\dim V$. Therefore, $S = S(E_k)$ for some $k \leq \dim V$. □

If S and T are two subspaces of an F-vector space V, then the intersection $S \cap T$ is again a subspace of F. However, the union $S \cup T$ is in general not a subspace. The smallest subspace containing $S \cup T$ is the **sum** $S + T$ of S and T:

$$S + T = \{v + w \mid v \in S, w \in T\}.$$

We have the following important dimension formula:

THEOREM 2.22 (Dimension Formula). *Let S and T be finite-dimensional subspaces of an F-vector space V. Then $S + T$ is finite-dimensional and*

$$\dim(S + T) = \dim S + \dim T - \dim(S \cap T).$$

PROOF. Let $\{v_1, \ldots, v_k\}$ be a basis of $S \cap T$. By Corollary 2.14, we can extend this basis to a basis

$$\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$$

of S and to a basis

$$\{v_1, \ldots, v_k, w_{k+1}, \ldots, w_m\}$$

of T. Clearly, the union of these two bases, which is

$$\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n, w_{k+1}, \ldots, w_m\},$$

generates $S+T$. We have to show that these vectors are linearly independent. Assume then that

$$a_1v_1 + \cdots + a_kv_k + a_{k+1}v_{k+1} + \cdots + a_nv_n + b_{k+1}w_{k+1} + \cdots + b_mw_m = 0.$$

This implies

$$a_1v_1 + \cdots + a_kv_k + a_{k+1}v_{k+1} + \cdots + a_nv_n = -b_{k+1}w_{k+1} - \cdots - b_mw_m.$$

The left hand side lies in S and the right hand side in T. Hence, both lie in $S \cap T$ and therefore can be written in terms of the basis $\{v_1, \ldots, v_k\}$:

$$a_1v_1+\cdots+a_kv_k+a_{k+1}v_{k+1}+\cdots+a_nv_n = -b_{k+1}w_{k+1}-\cdots-b_mw_m = c_1v_1+\cdots+c_kv_k.$$

However, the vectors $v_1, \dots, v_k, w_{k+1}, \dots, w_m$ are linearly independent, and therefore we must have $b_{k+1} = 0, \dots, b_m = 0, c_1 = 0, \dots, c_k = 0$. Finally, since the vectors $v_1, \dots, v_k, v_{k+1}, \dots, v_n$ are linearly independent, all the coefficients a_i are equal to 0 as well. □

Let us consider the special case that $S \cap T = (0)$, in which case we simply obtain $\dim(S + T) = \dim S + \dim T$:

LEMMA 2.23. *For two subspaces S and T, we have $S \cap T = (0)$ if and only if every $x \in S + T$ can be written as $x = v + w$, with $v \in S$ and $w \in T$, in one and only one way.*

PROOF. Let us assume first that $S \cap T = (0)$. If

$$x = v_1 + w_1 = v_2 + w_2$$

with $v_1, v_2 \in S$ and $w_1, w_2 \in T$, then

$$v_1 - v_2 = w_2 - w_1$$

lies in the intersection of S and T, hence is equal to 0, which proves uniqueness .

On the other hand, if $S \cap T \neq (0)$, then any nonzero vector $x \in S \cap T$ can be written as

$$x = x + 0 = 0 + x.$$

Therefore, if we put $v_1 = x, w_1 = 0$ and $v_2 = 0, w_2 = x$, then we get two different presentations of x. □

In the case that $S \cap T = (0)$, we call the sum $S + T$ a **direct sum** of S and T and denote it by $S \oplus T$. The concepts generalize to more than 2 summands:

DEFINITION 2.24. Let $S_1, \dots, S_k$ be subspaces of a vector space V. The **sum** $S_1 + \cdots + S_k$ is the subspace of V of all vectors x that can be written as

$$x = v_1 + v_2 + \cdots + v_k$$

with $v_i \in S_i$ for each $i = 1, \dots, k$.

It is sometimes convenient to write the sum using calculus notation:

$$S_1 + \cdots + S_k = \sum_{j=1}^{k} S_j.$$

The sum is called a **direct sum** if, for every vector $x \in S_1 + \cdots + S_k$, the above presentation is unique. If this is the case, then we write

$$S_1 \oplus S_2 \oplus \cdots \oplus S_k = \bigoplus_{j=1}^{k} S_j.$$

Lemma 2.23 easily generalizes to more than 2 summands as follows.

LEMMA 2.25. *Let $S_1, \dots, S_k$ be subspaces of a vector space V. Then*

$$S_1 + \cdots + S_k = S_1 \oplus \cdots \oplus S_k$$

if and only if, for each $i = 1, \dots, k$, we have

$$S_i \cap \Big(\sum_{\substack{j=1 \\ j \neq i}}^{k} S_j\Big) = (0).$$

EXAMPLE 2.26. Assume that $\{v_1, \dots, v_n\}$ is a set of generators of V. Then

$$V = Fv_1 \oplus Fv_2 \oplus \cdots \oplus Fv_n$$

if and only if $\{v_1, \dots, v_n\}$ is a basis of V.

We can use the dimension formula to prove the following result.

PROPOSITION 2.27. *For the direct sum of subspaces $S_1, \dots, S_k$ of a vector space V, we have*

$$\dim(S_1 \oplus S_2 \oplus \cdots \oplus S_k) = \dim S_1 + \dim S_2 + \cdots + \dim S_k.$$

PROOF. This follows by induction from the dimension formula. We write

$$S_1 \oplus S_2 \oplus \cdots \oplus S_k = S_1 \oplus (S_2 \oplus \cdots \oplus S_k).$$

The dimension formula implies that

$$\dim(S_1 \oplus S_2 \oplus \cdots \oplus S_k) = \dim S_1 + \dim(S_2 \oplus \cdots \oplus S_k).$$

Assuming that the result is true for a direct sum of $k-1$ subspaces, we have

$$\dim(S_2 \oplus \cdots \oplus S_k) = \dim S_2 + \cdots + \dim S_k,$$

hence the claim. □

Given any subspace S of a finite-dimensional vector space V, we can always find a subspace T such that $V = S \oplus T$. This is just a reformulation of the fact that a basis of S can be extended to a basis of V. That is, let $\{v_1, \dots, v_k\}$ be a basis of S and extend it to a basis

$$\{v_1, \dots, v_k, v_{k+1}, \dots, v_n\}$$

of V. Let T be the subspace with basis $\{v_{k+1}, \dots, v_n\}$. Then

$$\dim V = n = k + (n-k) = \dim S + \dim T.$$

Hence, by the dimension formula, $S \cap T = (0)$, which by Lemma 2.23 implies that $V = S \oplus T$. We note that the complementary subspace T is in general not uniquely determined since there are many ways of extending a basis of a subspace. We have shown the following.

PROPOSITION 2.28. *Given a subspace S of a finite-dimensional vector space V, there exists a subspace T of V such that $V = S \oplus T$.*

The concept of writing a vector space as a direct sum of subspaces of smaller dimensions will be important in the study of linear transformations.

CHAPTER 3

LINEAR TRANSFORMATIONS

1. Linear Transformations and Matrices

Let V and W be vector spaces over a field F.

DEFINITION 3.1. A map $T\colon V \to W$ is a **linear transformation** if

$$T(v_1 + v_2) = T(v_1) + T(v_2) \quad \text{and} \quad T(av) = aT(v)$$

for all $v, v_1, v_2 \in V$ and all $a \in F$.

In other words, T is a linear transformation if it respects vector addition and scalar multiplication. Definition 3.1 immediately implies that

$$T(a_1v_1 + a_2v_2 + \cdots + a_nv_n) = a_1T(v_1) + a_2T(v_2) + \cdots + a_nT(v_n).$$

In particular, this shows that if V is finite-dimensional with basis $\{v_1, \ldots, v_n\}$, then a linear transformation $T\colon V \to W$ is uniquely determined by the images

$$T(v_1), \ldots, T(v_n)$$

of the basis vectors, and these can be prescribed arbitrarily.

Attached to a linear transformation $T\colon V \to W$ are two subspaces: the **range** $T(V)$ of T,

$$T(V) = \{T(v) \mid v \in V\},$$

which is a subspace of W, and the **nullspace** $n(T)$ of T,

$$n(T) = \{v \in V \mid T(v) = 0\},$$

which is a subspace of V. The range of T is also called the **image** of T and denoted by $\mathrm{im}(T)$, and the nullspace of T is also called the **kernel** of T and denoted by $\ker(T)$.

If V is finite-dimensional, then we have the following relation between the dimensions of the image and the kernel of T.

PROPOSITION 3.2. *Assume that V is a finite-dimensional vector space and that $T\colon V \to W$ is a linear transformation. Then*

$$\dim n(T) \,+\, \dim T(V) = \dim V.$$

PROOF. By Proposition 2.28, we can choose a **complement** U of $n(T)$ in V, i.e., a subspace U of V such that

$$V = n(T) \oplus U.$$

Let $v_1, \ldots, v_k$ be a basis of $n(T)$, and let $v_{k+1}, \ldots, v_n$ be a basis of U. Clearly, the image vectors $T(v_{k+1}), \ldots, T(v_n)$ generate $T(V)$. We have to show that these vectors are linearly independent.

Assume that

$$a_{k+1}T(v_{k+1}) + a_{k+2}T(v_{k+2}) + \cdots + a_nT(v_n) = 0.$$

The left hand side equals $T(a_{k+1}v_{k+1} + \cdots + a_nv_n)$. Hence,

$$a_{k+1}v_{k+1} + \cdots + a_nv_n \in n(T) \cap U = (0).$$

This shows that $a_{k+1}v_{k+1} + \cdots + a_nv_n = 0$. It follows that $a_i = 0$ for $i = k+1, \ldots, n$, since the vectors $v_{k+1}, \ldots, v_n$ are linearly independent. Therefore,

$$\{T(v_{k+1}), \ldots, T(v_n)\}$$

is a basis for $T(V)$, and we obtain

$$\dim V = \dim n(T) + \dim U = \dim n(T) + \dim T(V),$$

as claimed. □

DEFINITION 3.3. A linear transformation $T\colon V \to W$ is **one-to-one** if

$$T(v_1) = T(v_2) \quad \Longrightarrow \quad v_1 = v_2$$

for any $v_1, v_2 \in V$. We say that T is **onto** if $T(V) = W$. A linear transformation T that is both one-to-one and onto is called an **isomorphism**.

We first note the following.

LEMMA 3.4. *The linear transformation T is one-to-one if and only if $n(T) = (0)$.*

PROOF. If T is one-to-one, then 0 is the only vector in V that is mapped to 0, so $n(T) = (0)$. Conversely, if $n(T) = (0)$ and $T(v_1) = T(v_2)$, then

$$T(v_1 - v_2) = T(v_1) - T(v_2) = 0,$$

so $v_1 - v_2$ is in $n(T)$, and therefore $v_1 = v_2$. □

LEMMA 3.5. *There exists an isomorphism $T\colon V \to W$ if and only if there exists an isomorphism $S\colon W \to V$.*

PROOF. Given T and $w \in W$, define $S(w)$ to be the unique vector $v \in V$ with $S(v) = w$. Note that v exists as T is onto, and it is unique as T is one-to-one. The converse follows in the same way. □

When the equivalent conditions of Lemma 3.5 hold, we call V and W **isomorphic** vector spaces. The particular isomorphism S constructed out of T in the proof of Lemma 3.5 is called the *inverse* of T and is denoted T^{-1}. In fact, the set of isomorphisms between isomorphic vector spaces forms a group under composition. Proposition 3.2 and Lemma 3.4 immediately imply:

COROLLARY 3.6. *Two finite-dimensional vector spaces over F are isomorphic if and only if they have the same dimension.*

We also note:

LEMMA 3.7. *If V and W are finite-dimensional and $\dim V = \dim W$, then the following statements are equivalent for a linear transformation $T\colon V \to W$:*

a. T is an isomorphism.

b. T is one-to-one.

c. T is onto.

EXAMPLES 3.8. 1. Differentiation $f \mapsto f'$ is a linear transformation from $P(\mathbb{R})$ to $P(\mathbb{R})$. This transformation is onto but not one-to-one, the nullspace being equal to $\mathbb{R}$. If we restrict to polynomials of degree $\leq n$, hence to $P_n(\mathbb{R})$, then the image is isomorphic to $P_{n-1}(\mathbb{R})$.

2. Integration $f \mapsto \int_a^b f(x)dx$ is a linear transformation from $P(\mathbb{R})$ to $\mathbb{R}$.

3. Integration $f \mapsto \int_0^x f(t)dt$ is a linear transformation from $P(\mathbb{R})$ to $P(\mathbb{R})$. It is one-to-one but not onto.

4. For any $m \times n$-matrix A, the map $x \mapsto Ax$ is a linear transformation from F^n to F^m. The nullspace of this transformation is equal to the nullspace of A and the image is equal to the column space of A.

5. Assume that V is n-dimensional, and let $B = \{v_1, \ldots, v_n\}$ be an *ordered basis* of V. (By "ordered", we mean simply that the elements of the basis are taken in a given order, the order in which they are listed.) The *coordinate map* $C_B : V \to F^n$ with respect B maps the ordered basis B to the standard ordered basis $\{e_1, \ldots, e_n\}$ of F^n. That is, $C_B(v_i) = e_i$ for $i = 1, \ldots, n$. The linear transformation C_B is clearly an isomorphism. If

$$v = a_1v_1 + \cdots + a_nv_n$$

is an arbitrary vector in V, then

$$C_B(v) = a_1e_1 + \cdots + a_ne_n = (a_1, \ldots, a_n).$$

We will usually view these vectors as column vectors in F^n.

The set $L(V, W)$ of all linear transformations from V to W becomes a vector space over F if we define the sum $S + T$ by

$$(S + T)(v) = S(v) + T(v)$$

and a scalar multiple aT by $(aT)(v) = aT(v)$.

Assume that $\dim V = n$ and $\dim W = m$. Let $B = \{v_1, \ldots, v_n\}$ be an ordered basis of V, and let $B' = \{w_1, \ldots, w_m\}$ be an ordered basis of W. We want to construct an isomorphism between the vector spaces $L(V, W)$ and $M_{mn}(F)$ which will depend on the choices of the bases B and B' and their orderings. To do this, we have to associate a matrix A to a given linear transformation $T\colon V \to W$. We consider the following diagram:

$$\begin{array}{ccc} V & \xrightarrow{T} & W \\ {\scriptstyle C_B}\downarrow & & \downarrow{\scriptstyle C_{B'}} \\ F^n & \xrightarrow[A\cdot]{} & F^m, \end{array}$$

and we want to define the matrix A so that multiplication by A makes the diagram commutative, i.e., we get the same result going from V to F^m in two different ways.

Let us start with a basis vector $v_j \in V$. Going along the top of the diagram, v_j is mapped to $T(v_j)$, which can be expressed in terms of the basis B' as

$$T(v_j) = a_{1j}w_1 + a_{2j}w_2 + \cdots + a_{mj}w_m.$$

The coordinate map $C_{B'}$ maps $T(v_j)$ to the column vector $(a_{1j}, a_{2j}, \ldots, a_{mj})$. Going the other way around, the coordinate map C_B maps v_j to the jth standard basis vector e_j of F^n (viewed as a column vector). Multiplying this vector by A gives the jth column of A. Therefore, this jth column has to be equal to $(a_{1j}, a_{2j}, \ldots, a_{mj})$. We see that the matrix A is equal to (a_{ij}). If we want to emphasize the dependence of A on T and the bases B, B', then we denote it by $A_T^{B,B'}$. It is now easy to verify that the map

$$T \mapsto A_T^{B,B'}$$

is linear and in fact an isomorphism between $L(V, W)$ and $M_{mn}(F)$:

PROPOSITION 3.9. *The linear map $T \mapsto A_T^{B,B'}$ from $L(V, W)$ to $M_{mn}(F)$ is an isomorphism. In particular, we have*

$$\dim L(V, W) = \dim V \cdot \dim W.$$

Assume that we have, in addition to T, a linear transformation $S\colon W \to U$, where U is an r-dimensional F-vector space with ordered basis B''. The situation is described by the following diagram:

$$\begin{array}{ccccc} V & \xrightarrow{T} & W & \xrightarrow{S} & U \\ {\scriptstyle C_B}\downarrow & & \downarrow{\scriptstyle C_{B'}} & & \downarrow{\scriptstyle C_{B''}} \\ F^n & \xrightarrow[A_T^{B,B'}]{} & F^m & \xrightarrow[A_S^{B',B''}]{} & F^r \end{array}$$

The composite linear transformation $S \circ T$, which is simply denoted by ST, maps V to U, and we have the following relation between the corresponding matrices:

$$A_{ST}^{B,B''} = A_S^{B',B''} \cdot A_T^{B,B'},$$

which simply means that the product of the transformations corresponds to the product of the matrices.

Let us specialize to the situation that $V = W$. In this case, we denote $L(V, V)$ simply by $L(V)$. In addition to being a vector space of dimension n^2 over F, where $\dim V = n$, we also have a product on $L(V)$ that turns $L(V)$ into a *ring*, isomorphic to the ring $M_n(F)$ of $n \times n$-matices over F.

If B and B' are ordered bases of V, then we can express a vector $v \in V$ in terms of the basis B and in terms of the basis B'. To obtain the matrix that describes the change of basis from B to B', we simply look at the special case that $T = 1$ is the identity transformation, and we write $A^{B,B'}$ instead of $A_1^{B,B'}$. In this case, the diagram looks like

$$\begin{array}{ccc} V & \xrightarrow{1} & V \\ {\scriptstyle C_B}\downarrow & & \downarrow{\scriptstyle C_{B'}} \\ F^n & \xrightarrow[A^{B,B'}.]{} & F^n, \end{array}$$

and we obtain

$$A^{B,B'} \cdot C_B(v) = C_{B'}(v)$$

for all $v \in V$. The ith column of $A^{B,B'}$ is simply the coordinate vector of the ith basis vector of B with respect to B'. The matrix $A^{B,B'}$ is invertible, and

$$\left(A^{B,B'}\right)^{-1} = A^{B',B}.$$

Let $T\colon V \to V$ be a linear transformation and B an ordered basis of V. We simply write A_T^B instead of $A_T^{B,B}$. To obtain the relationship between A_T^B and $A_T^{B'}$ for two ordered bases B and B' of V, we look at the diagram

$$\begin{array}{ccccccc} V & \xrightarrow{1} & V & \xrightarrow{T} & V & \xrightarrow{1} & V \\ {\scriptstyle C_{B'}}\downarrow & & \downarrow{\scriptstyle C_B} & & \downarrow{\scriptstyle C_B} & & \downarrow{\scriptstyle C_{B'}} \\ F^n & \xrightarrow[A^{B',B}\cdot]{} & F^n & \xrightarrow[A_T^B\cdot]{} & F^n & \xrightarrow[A^{B,B'}\cdot]{} & F^n \end{array}$$

and compare it to the diagram

$$\begin{array}{ccc} V & \xrightarrow{T} & V \\ {\scriptstyle C_{B'}}\downarrow & & \downarrow{\scriptstyle C_{B'}} \\ F^n & \xrightarrow[A_T^{B'}\cdot]{} & F^n \end{array}$$

We obtain

$$A_T^{B'} = \left(A^{B',B}\right)^{-1} \cdot A_T^B \cdot A^{B',B}.$$

In particular, we see that matrices describing a given linear transformation with respect to different bases are similar.

The task is now to find, for a given linear transformation $T\colon V \to V$, a "good" basis B of V so that the form of the matrix A_B^T is as simple as possible.

Example 3.10. Let $T\colon P_n(\mathbb{R}) \to P_n(\mathbb{R})$ be given by $T(f) = f'$. Let B be the ordered basis

$$B = \{1, x, x^2, \ldots, x^n\}.$$

The columns of the matrix A_T^B are obtained by expressing $T(1), T(x), \ldots, T(x^n)$ in terms of the basis B:

$$T(1) = 0, T(x) = 1, \ldots, T(x^i) = ix^{i-1}, \ldots, T(x^n) = nx^{n-1}.$$

This yields:

$$A_T^B = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 2 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & n \\ 0 & 0 & 0 & \ldots & 0 \end{bmatrix}$$

2. Minimal polynomials and invariant subspaces

Throughout, V denotes a finite-dimensional F-vector space, and $T\colon V \to V$ denotes a linear transformation. If

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m \in F[x]$$

is an arbitrary polynomial, then we denote by

$$f(T) = a_0\, 1 + a_1 T + \cdots + a_m T^m \in L(V)$$

the corresponding linear transformation obtained by substituting T for x, and if $A \in M_n(F)$, is an arbitrary $n \times n$-matrix, then we denote by

$$f(A) = a_0\, I_n + a_1 A + \cdots + a_m A^m \in M_n(F)$$

the corresponding matrix obtained by substituting A for x. If B is an ordered basis of V, and if A_T^B denotes the matrix corresponing to T under the isomorphism

$$L(V) \to M_n(F)$$

($n = \dim V$) described in the last section, then clearly $f(A_T^B)$ corresponds to $f(T)$. In particular, $f(T)$ is the zero transformation if and only if $f(A_T^B)$ is the zero matrix.

Since $L(V)$ has dimension n^2, where $n = \dim V$, the n^2+1 linear transformations

$$1, T, T^2, \ldots, T^{n^2}$$

are linearly dependent. Hence, there is a non-zero polynomial $f(x) \in F[x]$ of degree $\leq n^2$ such that $f(T) = 0$. Among all possible non-zero polynomials f with the property $f(T) = 0$, we choose one, denoted by $m_T(x)$, of smallest degree and assume it is monic.

Definition 3.11. We call $m_T(x)$ the **minimal polynomial** of the linear transformation T. Similarly, we define the minimal polynomial $m_A(x)$ for a matrix A. It is clear that $m_T(x) = m_A(x)$ whenever $A = A_T^B$ represents T with respect to a basis B.

The fact that $m_T(x)$ is uniquely determined by T can easily be seen from the following lemma.

Lemma 3.12. *If $f(x)$ is a non-zero polynomial such that $f(T) = 0$, then*

$$m_T(x) \mid f(x).$$

Proof. We use the Division Algorithm. That is,

$$f(x) = q(x) m_T(x) + r(x),$$

where either $r = 0$ or $\deg r(x) < \deg m_T(x)$. Inserting T for x, we obtain $r(T) = 0$ and, hence, $r = 0$ since the degree of $m_T(x)$ was minimal. The result follows. □

In general, it is not easy to find the minimal polynomial of a linear transformation. As we progress, we will see that the minimal polynomial $m_T(x)$ always divides the characteristic polynomial of T, which we denote by $c_T(x)$. We recall that

$$c_T(x) = \det(x - T)$$

can be computed as $\det(x \cdot I - A)$ using any matrix A representing T with respect to some basis B of V.

Here are some explicit examples:

EXAMPLES 3.13. 1. If $T = 0$ is the zero transformation, then $m_T(x) = x$.

2. If $T = 1$ is the identity, then $m_T(x) = x - 1$.

3. More generally, $T = c \cdot 1$ if and only if $m_T(x) = x - c$.

4. Let

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

be a 2×2-matrix. Then

$$A^2 - (a+d)A + (ad - bc)I_2 = 0,$$

which we can rewrite as

$$A^2 - \operatorname{tr}(A)A + \det(A)I_2 = 0.$$

If we assume that A is not a scalar multiple of the identity matrix, then $\deg m_A(x) = 2$, and therefore in these cases

$$m_A(x) = x^2 - \operatorname{tr}(A)x + \det(A).$$

We note that this is equal to the characteristic polynomial $c_A(x)$ of A.

Another family of examples arises as follows. Assume that W is a subspace of $V = \mathbb{R}^n$. We have

$$V = W \oplus W^\perp,$$

where $W^\perp$ is the orthogonal complement of V under the dot product. Every $v \in V$ can be written uniquely as

$$v = w + u$$

with $w \in W, u \in W^\perp$. The orthogonal projection of V on W is the linear transformation

$$P \colon V \to V, \quad P(w+u) = w.$$

The transformation P has the following property:

$$P^2 = P.$$

This property leads to the more general definition of a projection.

DEFINITION 3.14. A linear transformation $T \colon V \to V$ is a **projection** if $T^2 = T$.

We let $\operatorname{diag}(a_1, \ldots, a_r)$ denote the diagonal $r \times r$-matrix with with entires $a_1, \ldots, a_r$ along the diagonal.

PROPOSITION 3.15. *Assume that T is a projection, and let $k = \dim T(V)$. Then we have:*

i. $m_T(x) = x^2 - x = x(x-1)$ unless $k = 0$ or $k = \dim V$. In the latter cases, $T = 0$ or $T = 1$, so $m_T(x) = x$ or $m_T(x) = x - 1$, respectively.

ii. There exists a basis B of V such that

$$A_T^B = \operatorname{diag}(1, 1, \ldots, 1, 0, 0, \ldots, 0),$$

with k ones along the diagonal.

PROOF. We first show that

$$T(V) \cap n(T) = \{0\}.$$

Assume that $w \in T(V) \cap n(T)$. Then $w = T(v)$ for some $v \in V$, and $T(w) = 0$. We obtain

$$0 = T(w) = T^2(v) = T(v) = w.$$

Hence $w = 0$, as claimed. Proposition 3.2 then implies that

$$V = T(V) \oplus n(T).$$

We therefore have a basis

$$B = \{T(v_1), T(v_2), \ldots, T(v_k), v_{k+1}, \ldots, v_n\},$$

where $T(v_1), T(v_2), \ldots, T(v_k)$ are basis vectors for $T(V)$ and $v_{k+1}, \ldots, v_n$ are basis vectors for $n(T)$. Since $T(T(v_i)) = T(v_i)$ for $1 \leq i \leq k$, we obtain the result. □

DEFINITION 3.16. A subspace W of V is called T-**invariant** if $T(W) \subset W$. If W is a T-invariant subspace, then the **restriction** $T_W \in L(W)$ of T to W is simply defined by

$$T_W(w) = T(w)$$

for all $w \in W$.

Let us assume that we can decompose V into a direct sum

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$$

of T-invariant subspaces V_i. Let $T_i = T_{V_i}$ denote the restriction of T to V_i. If we choose ordered bases B_i for V_i, then

$$B = B_1 \cup B_2 \cup \ldots \cup B_r$$

is an ordered basis for V (taken in the order of the unions). The matrix $A = A_T^B$ of T with respect to B is **block diagonal**, which is to say that it looks like

$$A = \begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & A_r \end{bmatrix}$$

where the $A_i = A_{T_i}^{B_i}$ are the corresponding matrices for the restrictions T_i with respect to the bases B_i.

Let $m_T(x)$ and $c_T(x)$ denote the minimal and the characteristic polynomial of T, respectively, and let $m_i(x)$ and $c_i(x)$ denote the corresponding polynomials for T_i. The following result relates these polynomials.

LEMMA 3.17. *Let*

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$$

be a decomposition of V into T-invariant subspaces. Then

i. $c_T(x) = c_1(x)c_2(x)\cdots c_r(x)$.

ii. $m_T(x) = \operatorname{lcm}(m_1(x), m_2(x), \ldots, m_r(x))$.

PROOF. i. The matrix $x \cdot I - A$ is again block diagonal with blocks $x \cdot I - A_i$ along the diagonal. Since the determinant is multiplicative with respect to these blocks, we obtain part i.

ii. Let $m(x)$ denote the least common multiple of the polynomials

$$m_1(x), \ldots, m_r(x).$$

This means that each $m_i(x)$ divides $m(x)$ and that $m(x)$ is the monic polynomial of smallest degree with this property.

We first show that $m(T) = 0$. This is equivalent to showing that $m(T)(v) = 0$ for every basis vector $v \in B$. But if $v \in B_i$, then $m_i(T)(v) = m_i(T_i)(v) = 0$, and hence $m(T)(v) = 0$. This implies that $m_T(x) \mid m(x)$. Conversely, we clearly have $m_T(T_i)(v) = 0$ for all $v \in V_i$, so each $m_i(x) \mid m_T(x)$, and therefore $m(x) \mid m_T(x)$. Since both $m(x)$ and $m_T(x)$ are monic, they have to be equal.

□

To obtain T-invariant subspaces, we use the following lemma.

LEMMA 3.18. *Assume that $T\colon V \to V$ and $S\colon V \to V$ are linear transformations that commute, i.e., $ST = TS$. Then $S(V)$ and $n(S)$ are T-invariant.*

PROOF. Assume that $v \in S(V)$. Then $v = S(w)$ for some $w \in V$. Now

$$T(v) = T(S(w)) = S(T(w)) \in S(V),$$

which shows that $S(V)$ is T-invariant. Similarly, assume that $v \in n(S)$, i.e., $S(v) = 0$. Then

$$S(T(v)) = T(S(v)) = T(0) = 0,$$

so $n(S)$ is T-invariant. □

If $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$ is an arbitrary polynomial, then the linear transformation $S = f(T)$ commutes with T since

$$\begin{aligned} TS &= T(a_0 + a_1 T + \cdots + a_n T^n) \\ &= a_0 T + a_1 T^2 + \cdots + a_n T^{n+1} \\ &= (a_0 + a_1 T + \cdots + a_n T^n) T \\ &= ST, \end{aligned}$$

and therefore Lemma 3.18 implies:

COROLLARY 3.19. *For any polynomial $f(x) \in F[x]$, the range $f(T)(V)$ and the nullspace $n(f(T))$ of $f(T)$ are T-invariant subspaces of V.*

We now use this result to produce a decomposition of V into a direct sum of T-invariant subspaces according to the decomposition of the minimal polynomial $m_T(x)$ into a product of powers of irreducible polynomials.

THEOREM 3.20 (Primary Decomposition). *Let $T\colon V \to V$ be a linear transformation with minimal polynomial*

$$m_T(x) = p_1(x)^{e_1} p_2(x)^{e_2} \cdots p_r(x)^{e_r},$$

where $p_1(x), \ldots, p_r(x)$ are distinct irreducible polynomials. Then

$$V = n(p_1(T)^{e_1}) \oplus n(p_2(T)^{e_2}) \oplus \cdots \oplus n(p_r(T)^{e_r}).$$

PROOF. We prove the theorem by induction on the number r of powers of distinct irreducible polynomials in the decomposition of $m_T(x)$. If $r = 1$, then $m_T(x) = p(x)^e$ for some irreducible polynomial $p(x)$. Hence,

$$n(p(T)^e) = n(m_T(T)) = n(0) = V.$$

Let us assume now that the result is true for all linear transformations on finite-dimensional F-vector spaces for which the minimal polynomial factors into $r-1$ powers of distinct irreducible polynomials. We can write the given minimal polynomial

$$m_T(x) = p_1(x)^{e_1} p_2(x)^{e_2} \cdots p_r(x)^{e_r}$$

as

$$m_T(x) = q_1(x) q_2(x),$$

where $q_1(x) = p_1(x)^{e_1}$ and $q_2(x) = p_2(x)^{e_2} \cdots p_r(x)^{e_r}$. In particular, $q_1(x)$ and $q_2(x)$ are relatively prime. By Corollary 1.23, we find polynomials $a(x)$ and $b(x)$ for which

$$1 = a(x) q_1(x) + b(x) q_2(x),$$

and hence

$$1 = a(T) q_1(T) + b(T) q_2(T).$$

We want to show that

$$V = n(q_1(T)) \oplus n(q_2(T)).$$

Let $v \in V$. From above, we obtain

$$v = a(T) q_1(T)(v) + b(T) q_2(T)(v).$$

The vector $a(T) q_1(T)(v)$ is in the nullspace of $q_2(T)$ since

$$q_2(T) a(T) q_1(T)(v) = a(T) m_T(T)(v) = 0,$$

and similarly the vector $b(T) q_2(T)(v)$ is in the nullspace of $q_1(T)$. Therefore,

$$V = n(q_1(T)) + n(q_2(T)).$$

To show that the sum is direct, we have to show that $n(q_1(T)) \cap n(q_2(T)) = (0)$. But if $v \in n(q_1(T)) \cap n(q_2(T))$, then

$$v = a(T) q_1(T)(v) + b(T) q_2(T)(v) = 0 + 0 = 0.$$

Let T_1 and T_2 denote the restrictions of T to $n(q_1(T))$ and $n(q_2(T))$, respectively. From part ii of Lemma 3.17, we obtain $q_i(x) = m_{T_i}(x)$ for $i = 1, 2$. Our induction hypothesis implies that

$$n(q_2(T)) = n(p_2(T)^{e_2}) \oplus \cdots \oplus n(p_r(T)^{e_r}),$$

and hence

$$V = n(p_1(T)^{e_1}) \oplus n(p_2(T)^{e_2}) \oplus \cdots \oplus n(p_r(T)^{e_r}),$$

as claimed. □

This theorem has important consequences:

THEOREM 3.21. *A linear transformation $T\colon V \to V$ is diagonalizable if and only if the minimal polynomial $m_T(x)$ of T has the form*

$$m_T(x) = (x - \lambda_1)(x - \lambda_2)\cdots(x - \lambda_r)$$

with distinct elements $\lambda_1, \ldots, \lambda_r$ from F.

PROOF. We note that T is diagonalizable if and only if V has a basis consisting of eigenvectors of T. Let us assume first that T is diagonalizable, and let $\lambda_1, \ldots, \lambda_r$ denote the distinct eigenvalues of T. Let

$$m(x) = (x - \lambda_1)(x - \lambda_2)\cdots(x - \lambda_r).$$

We have to show that $m(x) = m_T(x)$. For each eigenvector v belonging to an eigenvalue λ_i, we have $(T - \lambda_i \cdot 1)v = 0$, and therefore $m(T)(v) = 0$. Since V has a basis consisting of eigenvectors of T, we obtain $m(T) = 0$. Therefore $m_T(x) \mid m(x)$. Let

$$m_i(x) = \frac{m(x)}{x - \lambda_i},$$

i.e., $m_i(x)$ is obtained from $m(x)$ by omitting the factor $x - \lambda_i$. Let v_i be an eigenvector belonging to λ_i. Then

$$m_i(T)(v_i) = \prod_{\substack{j=1 \\ j \neq i}}^{r} (T - \lambda_j \cdot 1)(v_i) = \prod_{\substack{j=1 \\ j \neq i}}^{r} (\lambda_i - \lambda_j)(v_i) \neq 0,$$

and therefore $m_i(T) \neq 0$ for all $i = 1, \ldots, r$. This implies that $m_T(x) = m(x)$.

Conversely, let us assume that

$$m_T(x) = (x - \lambda_1)(x - \lambda_2)\cdots(x - \lambda_r).$$

Theorem 3.20 implies that

$$V = n(T - \lambda_1 \cdot 1) \oplus n(T - \lambda_2 \cdot 1) \cdots \oplus n(T - \lambda_r \cdot 1).$$

Hence, V has a basis consisting of linearly independent vectors from $n(T - \lambda_i \cdot 1)$ for $i = 1, \ldots, r$. Since the non-zero vectors in $n(T - \lambda_i \cdot 1)$ are precisely the eigenvectors of T belonging to the eigenvalue λ_i, we see that V has a basis of eigenvectors, hence is diagonalizable. □

Theorem 3.21 shows that there are two possible forms of the minimal polynomial $m_T(x)$ of T which imply that T is *not* diagonalizable. First of all, $m_T(x)$ can have irreducible factors that are non-linear. E.g., over $\mathbb{R}$ the polynomial x^2+1 is irreducible. Hence, if $x^2 + 1$ divides the minimal polynomial $m_T(x)$ for a linear transformation $T\colon V \to V$, where V is a real vector space, then T is not diagonalizable. This happens for example, if $T\colon \mathbb{R}^2 \to \mathbb{R}^2$ is given by matrix multiplication by the matrix

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

In this case, the minimal polynomial is equal to x^2+1. We note that this case cannot happen if we consider vector spaces over the complex numbers $\mathbb{C}$.

The second form occurs if all irreducible factors of $m_T(x)$ are linear, but some divide $m_T(x)$ to a larger power than 1. In this case, the linear transformation can be

respresented by a matrix in *Jordan canonical form*, and we discuss this in the next section.

EXAMPLES 3.22. 1. Let us consider the linear transformation on $\mathbb{R}^6$ given by the following matrix

$$A = \begin{bmatrix} 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Then

$$A^2 = \begin{bmatrix} -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

and therefore

$$(A^2 + 1)(A^2 - 1) = 0.$$

This implies that the minimal polynomial $m_A(x) \in \mathbb{R}[x]$ divides $(x^2 + 1)(x^2 - 1)$. Since $A^2 - 1 \neq 0$, $m_A(x)$ has to contain the irreducible factor $x^2 + 1$. Since both $(A^2 + 1)(A + 1)$ and $(A^2 + 1)(A - 1)$ are non-zero matrices, the minimal polynomial is actually equal to $(x^2 + 1)(x^2 - 1) = (x^2 + 1)(x + 1)(x - 1)$:

$$m_A(x) = (x^2 + 1)(x + 1)(x - 1).$$

This is the factorization of $m_A(x)$ into a product of distinct irreducible polynomials in $\mathbb{R}[x]$. Theorem 3.20 implies that A is not diagonalizable over $\mathbb{R}$. According to Theorem 3.20, the primary decomposition of the vector space $\mathbb{R}^6$ looks like

$$\mathbb{R}^6 = n(A^2 + 1) \oplus n(A + 1) \oplus n(A - 1).$$

Now, $A^2 + 1$ has rank 2. Thus, $n(A^2 + 1)$ has dimension 4, and the other two nullspaces have both dimension 1 and are in fact the eigenspaces belonging to the eigenvalues -1 and 1, respectively. An eigenvector for -1 is given by $e_5 - e_6$, and an eigenvector for 1 is given by $e_5 + e_6$. The nullspace $n(A^2 + 1)$ of $A^2 + 1$ has a basis $\{e_1, e_2, e_3, e_4\}$. The direct sum decomposition of $\mathbb{R}^6$ then simply corresponds to the basis $\{e_1, e_2, e_3, e_4, e_5 - e_6, e_5 + e_6\}$ of $\mathbb{R}^6$. We note that $n(A^2+1)$ decomposes further into a direct sum of A-invariant subspaces

$$n(A^2 + 1) = S(e_1, e_2) \oplus S(e_3, e_4),$$

which is *not* a consequence of the primary decomposition.

2. Let us look at the linear transformation on $\mathbb{R}^3$ given by the matrix

$$A = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & 2 \end{bmatrix}.$$

We compute the powers

$$A^2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & -1 & -2 \\ 1 & 2 & 3 \end{bmatrix}$$

and

$$A^3 = \begin{bmatrix} 0 & 0 & 0 \\ -1 & -2 & -3 \\ 2 & 3 & 4 \end{bmatrix}$$

and obtain the relation

$$A^3 - 2A^2 + A = 0.$$

Therefore, the minimal polynomial $m_A(x) \in \mathbb{R}[x]$ divides $x^3 - 2x^2 + x = x(x-1)^2$. It is easy to verify that $A \neq 0$, $A - 1 \neq 0$, $(A-1)^2 \neq 0$, and $A(A-1) \neq 0$, so that the minimal polynomial is equal to $x(x-1)^2$:

$$m_A(x) = x(x-1)^2.$$

Again, A is not diagonalizable by Theorem 3.20, and the primary decomposition is

$$\mathbb{R}^3 = n(A) \oplus n((A-1)^2).$$

The subspace $n(A)$ is 1-dimensional and is simply the eigenspace belonging to the eigenvalue 0. A basis vector for $n(A)$ is, e.g., given by the eigenvector $(1, -2, 1)$. Now we compute

$$(A-1)^2 = \begin{bmatrix} 1 & 0 & 0 \\ -2 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

The dimension of the nullspace $n((A-1)^2)$ is equal to 2, and a basis is given, e.g., by the basis vectors e_2 and e_3. Again, this is not the best choice of a basis for $n((A-1)^2)$. We choose $e_2 = (0, 1, 0)$, which is not in the eigenspace $n(A-1)$ belonging to the eigenvalue 1 of A. We compute $(A-1)e_2 = (0, -1, 1)$, which is now an eigenvector for the eigenvalue 1, and take as our basis of $\mathbb{R}^3$:

$$B = \{(1, -2, 1), (0, -1, 1), (0, 1, 0)\}.$$

With respect to this basis, the matrix A is represented by

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix},$$

which is in *Jordan canonical form*. In the next section we will see that this always works if the minimal polynomial splits into a product of linear factors.

3. The Jordan canonical form

We continue to assume in this section that V denotes a finite-dimensional F-vector space and that $T\colon V \to V$ is a linear transformation. We want to consider the special case that all irreducible factors of the minimal polynomial $m_T(x)$ are linear, i.e., we assume that

$$m_T(x) = (x - \lambda_1)^{e_1}(x - \lambda_2)^{e_2} \cdots (x - \lambda_r)^{e_r},$$

where the λ_i are distinct elements from F. We note that this is always true if $F = \mathbb{C}$ is the field of complex numbers.

According to Theorem 3.20, we have the following decomposition of V as a direct sum of T-invariant subspaces:

$$V = n((T-\lambda_1)^{e_1}) \oplus n((T-\lambda_2)^{e_2}) \oplus \cdots \oplus n((T-\lambda_r)^{e_r}).$$

Let T_i denote the restriction of T to the subspace $n((T-\lambda_i)^{e_i})$ of V. From Lemma 3.17, we know that the minimal polynomial of T_i is equal to $(x-\lambda_i)^{e_i}$:

$$m_{T_i}(x) = (x-\lambda_i)^{e_i}.$$

LEMMA 3.23. *The only eigenvalue of T_i is λ_i.*

PROOF. Let us first show that λ_i is in fact an eigenvalue. This follows since

$$n(T-\lambda_i) \subset n((T-\lambda_i)^{e_i}),$$

and any non-zero vector in $n(T-\lambda_i)$ is an eigenvector for λ_i.

Conversely, let us assume that v is an eigenvector for the eigenvalue λ of T_i. Thus

$$T_i v = \lambda v.$$

This implies that

$$T_i^k v = \lambda^k v$$

for all $k \geq 1$ and, more generally,

$$f(T_i)v = f(\lambda)v$$

for all polynomials $f(x) \in F[x]$. Taking $f(x) = (x-\lambda_i)^{e_i}$, we obtain

$$(T_i - \lambda_i)^{e_i} v = 0 = (\lambda - \lambda_i)^k v.$$

Hence, $\lambda = \lambda_i$ since $v \neq 0$. □

We obtain the following corollary.

COROLLARY 3.24. *Assume that*

$$m_T(x) = (x-\lambda_1)^{e_1}(x-\lambda_2)^{e_2}\cdots(x-\lambda_r)^{e_r}.$$

Then the λ_i, $1 \leq i \leq r$, are precisely the distinct eigenvalues of T.

PROOF. It follows from Lemma 3.23 that every λ_i is an eigenvalue of T. Let us assume now that λ is an eigenvalue of T, and let v be an eigenvector belonging to λ. Then we can write v uniquely as

$$v = v_1 + v_2 + \cdots + v_r,$$

where $v_i \in n((T-\lambda_i)^{e_i})$ for $1 \leq i \leq r$. Applying T, we obtain

$$Tv = Tv_1 + Tv_2 + \cdots + Tv_r = \lambda v = \lambda v_1 + \lambda v_2 + \cdots + \lambda v_r.$$

Since V is a direct sum of the subspaces $n((T-\lambda_i)^{e_i})$, and since these are T-invariant, we must have

$$Tv_i = \lambda v_i$$

for all i. Now $v \neq 0$, and therefore at least one of the v_i's is non-zero, hence an eigenvector of T_i for the eigenvalue λ. Lemma 3.23 implies that $\lambda = \lambda_i$. □

DEFINITION 3.25. The T-invariant subspaces

$$E_{\lambda_i} = n((T - \lambda_i)^{e_i})$$

of V are called **generalized eigenspaces** of T.

Because of the Primary Decomposition Theorem, we can concentrate now on the situation that

$$m_T(x) = (x - \lambda)^e.$$

Then

$$V = E_\lambda = n((T - \lambda)^e).$$

The linear transformation $N = T - \lambda$ now has the property that $N^e = 0$. Linear transformations of this kind have a special name:

DEFINITION 3.26. A linear transformation $N : V \to V$ is called **nilpotent** if $N^e = 0$ for some $e \geq 1$. The smallest integer $m \geq 1$ such that $N^m = 0$ is called the **index of nilpotency** of N.

In our case, $N = T - \lambda$ is nilpotent of index e.

If $B = \{v_1, v_2, \ldots, v_n\}$ is an ordered basis of V, then we get the following relation between the matrices A_N^B and A_T^B describing N and T with respect to B:

$$A_T^B = \lambda I_n + A_N^B.$$

We also note that a subspace U of V is T-invariant if and only if U is N-invariant. In fact, if U is T-invariant, then for all $u \in U$ we have $Tu \in U$, so $Nu = Tu - \lambda u \in U$, and conversely. We wish to find a "nice" basis B of V with A_N^B is as simple as possible.

Assume that N is a nilpotent transformation on V of index e. The smallest N-invariant subspaces can be constructed as follows. Let $v \in V$ be any non-zero vector. If U is an N-invariant subspace of V containing v, then U contains $v, Nv, N^2v, \ldots$. Let k be the smallest positive integer so that $N^k v = 0$. Then U contains the span $S(v, Nv, \ldots, N^{k-1}v)$. We claim that this span is already N-invariant and has basis $v, Nv, \ldots, N^{k-1}v$.

LEMMA 3.27. *Let N be a nilpotent transformation and $v \neq 0$. Let k be the smallest integer so that $N^k v = 0$. Then $v, Nv, \ldots, N^{k-1}v$ are linearly independent, and $S(v, Nv, \ldots, N^{k-1}v)$ is N-invariant.*

PROOF. Assume that

$$a_0 v + a_1 Nv + \cdots + a_{k-1} N^{k-1} v = 0,$$

and let us assume that i is the smallest index so that $a_i \neq 0$. We apply N^{k-i-1}. Then

$$a_i N^{k-1} v + a_{i+1} N^k v + \cdots a_{k-1} N^{2(k-1)-i} v = 0.$$

But $N^k v = 0$, hence $N^m v = 0$ for all $m \geq k$, and therefore

$$a_i N^{k-1} v = 0.$$

Since $N^{k-1} v \neq 0$, we obtain $a_i = 0$, a contradiction. Therefore, our assumption that one of the a_i's is non-zero was wrong, which proves linear independence.

Since $N^k v = 0$, the span $S(v, Nv, \ldots, N^{k-1}v)$ is clearly N-invariant. □

DEFINITION 3.28. The N-invariant subspaces $S(v, Nv, \ldots, N^{k-1}v)$ are denoted by $\langle v \rangle$ and called **cyclic** subspaces of V. We note that they depend on N and are of dimension k, where k is the smallest integer for which $N^k v = 0$.

If we restrict our attention now to a single cyclic subspace, then we obtain a very "nice" matrix representation:

LEMMA 3.29. *Assume N is a nilpotent transformation on a cyclic space $\langle v \rangle$ of dimension k. Then the $k \times k$-matrix A_N^B representing N with respect to the basis*

$$B = \{N^{k-1}v, N^{k-2}v, \ldots, Nv, v\}$$

has the form

$$A_N^B = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & 1 \\ 0 & \cdots & 0 & 0 & 0 \end{bmatrix}.$$

PROOF. The first basis vector is mapped under N to $N^k v = 0$, and all the other ones are mapped to their predecessors, hence the result. □

REMARK 3.30. Of course, one could use the basis $\{v, Nv, \ldots, N^{k-1}v\}$ instead. This gives a matrix with all the 1's below the diagonal instead of above the diagonal. The use of the basis B is more consistent with the literature.

Our final task is now to show that, in fact, our vector space V can be written as a direct sum of cyclic subspaces. The following approach is constructive and actually produces generators for the cyclic subspaces. We continue to assume that $N : V \to V$ is nilpotent of index e.

We have a sequence of subspaces

$$(0) = n(N^0) \subset n(N) \subset n(N^2) \subset \cdots \subset n(N^e) = V.$$

We claim that these inclusions are strict. In fact, let us assume that $n(N^i) = n(N^{i+1})$ for some $i \leq e - 1$. Let $v \in V = n(N^e)$. Then

$$N^e v = N^{i+1} N^{e-i-1} v = 0,$$

and hence

$$N^{e-i-1} v \in n(N^{i+1}) = n(N^i).$$

Therefore,

$$N^i N^{e-i-1} v = N^{e-1} v = 0,$$

which implies that $V = n(N^{e-1})$, and therefore the index of nilpotency for N is $e-1$. This is a contradiction, so

$$n(N^i) \subsetneq n(N^{i+1})$$

for all i, $0 \leq i \leq e - 1$.

We now choose, for each $1 \leq i \leq e$, any complement W_i of $n(N^{i-1})$ in $n(N^i)$, so

$$n(N^i) = n(N^{i-1}) \oplus W_i.$$

Clearly, $W_1 = n(N)$ since $n(N^0) = \{0\}$.

LEMMA 3.31. *For $i \geq 2$, we have:*

i. $N(W_i) \cap n(N^{i-2}) = \{0\}$.

ii. The restriction of N to W_i is one-to-one.

PROOF. i. Let $v \in N(W_i)$, so that $v = Nw$ for some $w \in W_i$. If $v \in n(N^{i-2})$ as well, then by definition

$$0 = N^{i-2}v = N^{i-1}w,$$

and therefore $w \in n(N^{i-1})$. Hence

$$w \in n(N^{i-1}) \cap W_i = \{0\}.$$

This implies that $v = 0$.

ii. Let $v \in W_i$, and assume that $Nv = 0$. Since $i \geq 2$, we have $n(N) \subset n(N^{i-1})$, and therefore

$$v \in W_i \cap n(N) \subset W_i \cap n(N^{i-1}) = \{0\}.$$

This shows that N is one-to-one on W_i.

□

We are now ready to construct special complements W_i for $1 \leq i \leq e$. For W_e, we can take any complement of $n(N^{e-1})$ in V:

$$V = n(N^e) = n(N^{e-1}) \oplus W_e.$$

If $e = 1$, we can stop since $N = 0$ in this case and $W_1 = V$. Otherwise, $e \geq 2$, and we can proceed inductively downwards from $i = e - 1$. That is, take $i \leq e - 1$, and assume we have already defined W_{i+1}. We know from Lemma 3.31i that

$$N(W_{i+1}) \cap n(N^{i-1}) = \{0\}.$$

We then define W_i via

$$W_i = N(W_{i+1}) \oplus U_i,$$

where U_i is chosen so that

$$n(N^i) = n(N^{i-1}) \oplus N(W_{i+1}) \oplus U_i.$$

Note that for $i = 1$ we simply have

$$n(N) = N(W_2) \oplus U_1.$$

If we unwind all the successive definitions and put $U_e = W_e$, then we can rewrite

$$W_i = N^{e-i}(U_e) \oplus N^{e-1-i}(U_{e-1}) \oplus \cdots \oplus N(U_{i+1}) \oplus U_i.$$

We observe that

$$\begin{aligned} V &= n(N^e) \\ &= n(N^{e-1}) \oplus W_e \\ &= n(N^{e-2}) \oplus W_{e-1} \oplus W_e \\ &\vdots \\ &= W_1 \oplus W_2 \oplus \cdots \oplus W_e, \end{aligned}$$

and therefore

$$V = \left\{ \begin{array}{ccccccccccc} & & U_e & & & & & & & & \\ \oplus & & N(U_e) & \oplus & U_{e-1} & & & & & & \\ \oplus & & N^2(U_e) & \oplus & N(U_{e-1}) & \oplus & U_{e-2} & & & & \\ \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & & & & \\ \oplus & & N^{e-1}(U_e) & \oplus & N^{e-2}(U_{e-1}) & \oplus & N^{e-3}(U_{e-2}) & \oplus \cdots \oplus & N(U_2) & \oplus & U_1 \end{array} \right\}.$$

We can now read the above direct sum decomposition for V vertically: a typical summand looks like

$$U_i \oplus N(U_i) \oplus N^2(U_i) \oplus \cdots \oplus N^{i-1}(U_i).$$

If $\{w_1, w_2, \ldots, w_m\}$ is a basis of U_i, then by Lemma 3.31ii,

$$\{N^k w_1, N^k w_2, \ldots, N^k w_m\}$$

is a basis for $N^k(U_i)$ for $1 \leq k \leq i-1$. Since $N^i(U_i) = 0$ by definition,

$$\langle w_1 \rangle \oplus \langle w_2 \rangle \oplus \cdots \oplus \langle w_m \rangle$$

is a decomposition of

$$U_i \oplus N(U_i) \oplus N^2(U_i) \oplus \cdots \oplus N^{i-1}(U_i)$$

into a direct sum of cyclic subspaces. Letting i run from 1 to e, we obtain a decomposition of V into a direct sum of cyclic subspaces. We have shown the first part of the following theorem:

THEOREM 3.32. *Let $N : V \to V$ be a nilpotent transformation. Then:*

a. V decomposes into a direct sum of cyclic subspaces $\langle v_i \rangle$:

$$V = \langle v_1 \rangle \oplus \langle v_2 \rangle \oplus \cdots \oplus \langle v_t \rangle.$$

b. The number t and the dimensions of the cyclic subspaces $\langle v_i \rangle$ are uniquely determined by N and V.

PROOF. We only have to prove part b, which we do using induction on the index of nilpotency e of N. If $e = 1$, then $N = 0$, the $\langle v_i \rangle$ are 1-dimensional, and their number is equal to the dimension of V.

We assume now that the statement is true for all nilpotent transformations $W \to W$ of index $\leq e-1$ on all finite-dimensional F-vector spaces W, and we consider $N : V \to V$ of index $e > 1$. Let

$$V = \langle v_1 \rangle \oplus \langle v_2 \rangle \oplus \cdots \oplus \langle v_t \rangle$$

be a decomposition of V into cyclic subspaces with respect to N. Let e_i denote the index of nilpotency of the restriction of N to the cyclic subspace $\langle v_i \rangle$, i.e.,

$$N^{e_i} v_i = 0, \quad N^{e_i - 1} v_i \neq 0.$$

Rearranging the order of the cyclic subspaces, if necessary, we may assume that $e_1 = 1, \ldots, e_s = 1$, and $e_i > 1$ for $i > s$. The nullspace of N is equal to

$$n(N) = \langle v_1 \rangle \oplus \cdots \langle v_s \rangle \oplus \langle N^{e_{s+1}-1} v_{s+1} \rangle \oplus \cdots \oplus \langle N^{e_t - 1} v_t \rangle.$$

We see that the number t of cyclic summands is uniquely determined by the nullity of N:

$$t = \dim n(N).$$

Next, observe that the image of N decomposes as

$$N(V) = \langle Nv_{s+1}\rangle \oplus \cdots \oplus \langle Nv_t\rangle.$$

On $W = N(V)$, the linear transformation $N : W \to W$ has index of nilpotency equal to $e-1$. By induction hypothesis, the number $t-s$ of cyclic summands of W and their dimensions are uniquely determined. This implies that the number s of one-dimensional cyclic summands in V is uniquely determined. Furthermore, for $i \geq s+1$, we have

$$\dim\langle v_i\rangle = \dim\langle Nv_i\rangle + 1,$$

so these dimensions are also uniquely determined. □

Let us go back to our original situation that $T\colon V \to V$ is a linear transformation, and we assume that the minimal polynomial $m_T(x)$ splits into linear factors:

$$m_T(x) = (x-\lambda_1)^{e_1}(x-\lambda_2)^{e_2}\cdots(x-\lambda_r)^{e_r}.$$

Corollary 3.24 shows that $\lambda_1, \ldots, \lambda_r$ are precisely the distinct eigenvalues of T. On each generalized eigenspace $E_{\lambda_i} = n((T-\lambda_i)^{e_i})$, the linear transformation $N_i = T-\lambda_i$ is nilpotent of index e_i. According to Theorem 3.32, each E_{λ_i} splits further into a direct sum of N_i-invariant subspaces that are cyclic for N_i. These subspaces are T-invariant, and by Lemma 3.29, T can on each of them be represented by a square matrix of the form

$$\begin{bmatrix} \lambda_i & 1 & 0 & \cdots & 0 \\ 0 & \lambda_i & 1 & \ddots & \vdots \\ 0 & 0 & \lambda_i & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & 1 \\ 0 & \cdots & 0 & 0 & \lambda_i \end{bmatrix}.$$

These specific matrices are called **Jordan matrices** or **Jordan blocks**. They are determined by the diagonal entry λ_i and their size. What we have shown then is the following result known as **Jordan decomposition** of T or **Jordan canonical form**:

THEOREM 3.33 (Jordan canonical form). *Let $T\colon V \to V$ be a linear transformation with minimal polynomial $m_T(x)$ of the form*

$$m_T(x) = (x-\lambda_1)^{e_1}(x-\lambda_2)^{e_2}\cdots(x-\lambda_r)^{e_r}.$$

There exists an ordered basis B of V such that T is represented with respect to the basis B by a matrix of the form

$$A_T^B = \begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & A_r \end{bmatrix},$$

where each A_i is a block matrix with Jordan blocks of the form

$$\begin{bmatrix} \lambda_i & 1 & 0 & \cdots & 0 \\ 0 & \lambda_i & 1 & \ddots & \vdots \\ 0 & 0 & \lambda_i & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & 1 \\ 0 & \cdots & 0 & 0 & \lambda_i \end{bmatrix}.$$

along the diagonal.

The number of Jordan blocks and their sizes are uniquely determined by T.

Obviously, the Jordan matrices are specified by their size and by the diagonal entry. Therefore the following notation is useful:

$$J_k(\lambda) = \begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \ddots & \vdots \\ 0 & 0 & \lambda & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & 1 \\ 0 & \cdots & 0 & 0 & \lambda \end{bmatrix},$$

where the matrix is of size $k \times k$.

If $\lambda = \lambda_i$ is one of the eigenvalues of T and $A = A_i$ is the matrix block belonging to the generalized eigenspace E_{λ_i}, then A has the form

$$A = \begin{bmatrix} J_{k_1}(\lambda) & 0 & \cdots & 0 \\ 0 & J_{k_2}(\lambda) & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & J_{k_t}(\lambda) \end{bmatrix}$$

for some positive integers $k_1, \ldots, k_t$. It is customary to write the Jordan blocks in decreasing order, i.e., assume that $k_1 \geq k_2 \geq \cdots \geq k_t$.

We can extract the following facts from the proof of Theorem 3.32.

COROLLARY 3.34. *Let $T\colon V \to V$ be a linear transformation with minimal polynomial $m_T(x)$ of the form*

$$m_T(x) = (x - \lambda_1)^{e_1}(x - \lambda_2)^{e_2} \cdots (x - \lambda_r)^{e_r}.$$

For each eigenvalue λ_i, the following hold:

a. The side length of the largest Jordan block belonging to λ_i is equal to e_i.

b. The number of Jordan blocks belonging to λ_i is equal to the dimension of the eigenspace $n(T - \lambda_i)$, the geometric multiplicity of λ_i.

Another consequence of the Jordan decomposition is the following theorem of Cayley-Hamilton:

THEOREM 3.35 (Cayley-Hamilton). *Let $T\colon V \to V$ be a linear transformation with minimal polynomial $m_T(x)$ of the form*

$$m_T(x) = (x - \lambda_1)^{e_1}(x - \lambda_2)^{e_2} \cdots (x - \lambda_r)^{e_r}.$$

The minimal polynomial $m_T(x)$ divides the characteristic polynomial $c_T(x)$:

$$m_T(x) \mid c_T(x),$$

in particular

$$c_T(T) = 0.$$

PROOF. We know that V decomposes into a direct sum of cyclic subspaces:

$$V = \langle v_1 \rangle \oplus \langle v_2 \rangle \oplus \cdots \oplus \langle v_s \rangle.$$

On each subspace $\langle v_i \rangle$, the minimal polynomial and the characteristic polynomial of the restriction T_i of T are identical:

$$m_{T_i}(x) = c_{T_i}(x).$$

By Lemma 3.17, the minimal polynomial $m_T(x)$ is the least common multiple of the $m_{T_i}(x)$'s, whereas the characteristic polynomial $c_T(x)$ is the product of the $c_{T_i}(x)$'s. Therefore, $m_T(x) \mid c_T(x)$. Since $m_T(T) = 0$, the same is true for $c_T(T)$. □

Here are some examples:

EXAMPLES 3.36. a. Consider the linear transformation $N : \mathbb{R}^5 \to \mathbb{R}^5$ defined by

$$N(x_1, x_2, x_3, x_4, x_5) = (0, x_3 + x_4, 0, x_3, x_1 + x_4).$$

Let us compute the powers:

$$N^2(x_1, x_2, x_3, x_4, x_5) = (0, x_3, 0, 0, x_3),$$

$$N^3(x_1, x_2, x_3, x_4, x_5) = (0, 0, 0, 0, 0).$$

Therefore, N is nilpotent of index 3.

To find the Jordan decomposition according to the procedure described in Theorem 3.32, we have to find the dimensions and bases of the two subspaces $n(N^2)$ and $n(N)$. We note that the standard basis vectors e_1, e_2, e_4, e_5 form a basis of $n(N^2)$, and the basis vectors e_2, e_5 form a basis of $n(N)$.

From our basis of $n(N^2)$, we know that

$$\mathbb{R}^5 = n(N^2) \oplus S(e_3),$$

so we can take for U_3 the 1-dimensional subspace spanned by e_3. This produces the first cyclic summand $\langle e_3 \rangle$ of $\mathbb{R}^5$ with basis

$$N^2 e_3, N e_3, e_3.$$

Now,

$$N e_3 = (0, 1, 0, 1, 0) = e_2 + e_4.$$

Therefore,

$$n(N^2) = n(N) \oplus N(U_3) \oplus U_2 = S(e_2, e_5) \oplus S(e_2 + e_4) \oplus U_2.$$

We can take

$$U_2 = S(e_1)$$

and obtain the second cyclic summand $\langle e_1 \rangle$ of $\mathbb{R}^5$ with basis

$$N e_1, e_1.$$

The decomposition of $\mathbb{R}^5$ is then

$$\mathbb{R}^5 = \langle e_3 \rangle \oplus \langle e_1 \rangle,$$

and the Jordan canonical form of N with respect to the ordered basis

$$\{N^2 e_3, N e_3, e_3, N e_1, e_1\}$$

is

$$\left[\begin{array}{ccc:cc} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

b. In this example, we consider the linear transformation $T\colon \mathbb{R}^3 \to \mathbb{R}^3$ defined by

$$T(x, y, z) = (5x + 4y + 3z, -x - 3z, x - 2y + z).$$

With respect to the standard basis of $\mathbb{R}^3$, the matrix representation of T is given by

$$A = \begin{bmatrix} 5 & 4 & 3 \\ -1 & 0 & -3 \\ 1 & -2 & 1 \end{bmatrix}.$$

The characteristic polynomial of T is

$$c_T(x) = \det(x - A) = \det \begin{bmatrix} x-5 & -4 & -3 \\ 1 & x & 3 \\ -1 & 2 & x-1 \end{bmatrix} = (x-4)^2(x+2),$$

and therefore we have two eigenvalues $\lambda_1 = 4$ and $\lambda_2 = -2$.

Let us look at the eigenspace

$$E_{\lambda_1} = n(A - 4) = n\left(\begin{bmatrix} 1 & 4 & 3 \\ -1 & -4 & -3 \\ 1 & -2 & -3 \end{bmatrix}\right),$$

which is 1-dimensional.

This information is already sufficient to determine the Jordan canonical form. That is, A is similar to

$$\begin{bmatrix} 4 & 1 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & -2 \end{bmatrix}.$$

To obtain a basis B that produces the Jordan canonical form, we need a basis for E_{λ_1}, hence a basis of the nullspace of

$$(A - 4)^2 = \begin{bmatrix} 0 & -18 & -18 \\ 0 & 18 & 18 \\ 0 & 18 & 18 \end{bmatrix}.$$

We have

$$n((A-4)^2) = n(A-4) \oplus U_2,$$

where U_2 is 1-dimensional and can be chosen to be spanned by $v = (0, 1, -1)$ since

$$(A-4)v = (1, -1, 1) \neq 0.$$

Finally, it is easy to see that $(1, -1, -1)$ is an eigenvector for $\lambda_2 = -2$. Therefore $\{(1, -1, 1), (0, 1, -1), (1, -1, 1)\}$ is a basis for $\mathbb{R}^3$ that produces the Jordan canonical form.

REMARK 3.37. We restricted our attention in this section to linear transformations $T\colon V \to V$, with V a finite-dimensional F-vector space, for which the minimal polynomial $m_T(x)$ splits into a product of linear factors. If $F = \mathbb{C}$ then this is not a restriction, but in general it is. In the general case, one can still obtain a canonical form, the **rational canonical form**, which is more complicated than the Jordan canonical form but nevertheless determines the linear transformation T uniquely up to permuting blocks in the matrix presentation. It is also true in general that the minimal polynomial $m_T(x)$ divides the characteristic polynomial $c_T(x)$, and therefore the Cayley-Hamilton theorem holds in general:

$$c_T(T) = 0.$$

For more details, see Appendix A.

The main application of the Jordan canonical form is to solve homogeneous systems of linear differential equations over the complex numbers. Recall that this means that we try to find functions $y_1(t), y_2(t), \ldots, y_n(t)$ such that

$$\begin{aligned}
y_1'(t) &= a_{11}y_1(t) + a_{12}y_2(t) + \cdots + a_{1n}y_n(t) \\
y_2'(t) &= a_{21}y_1(t) + a_{22}y_2(t) + \cdots + a_{2n}y_n(t) \\
&\vdots \qquad\qquad\qquad \vdots \\
y_n'(t) &= a_{n1}y_1(t) + a_{n2}y_2(t) + \cdots + a_{nn}y_n(t)
\end{aligned}$$

or, in matrix form,

$$y'(t) = A\,y(t),$$

where $A = (a_{ij})$ is a complex $n \times n$-matrix and $y(t) = (y_1(t), y_2(t), \ldots, y_n(t))$. The main result on the Jordan canonical form tells us that we can find an invertible matrix P such that

$$P^{-1}AP = B$$

is in Jordan form. We obtain

$$P^{-1}y'(t) = P^{-1}AP\,P^{-1}y(t) = B\,P^{-1}y(t).$$

Let $z(t) = P^{-1}y(t)$. Then clearly $z'(t) = P^{-1}y'(t)$, and the new system reads

$$z'(t) = Bz(t).$$

Once we solve this system for $z(t)$, then we find the solutions $y(t)$ to the original system simply as

$$y(t) = Pz(t).$$

Since B is composed of Jordan blocks along the diagonal, we only have to solve the system for a single Jordan block $J_k(a)$, i.e., to look at an equation

$$z'(t) = J_k(a)z(t).$$

This system reads explicitly

$$\begin{array}{rcl} z_1'(t) & = & az_1(t) + z_2(t) \\ z_2'(t) & = & az_2(t) + z_3(t) \\ \vdots & & \vdots \\ z_{k-1}'(t) & = & az_{k-1}(t) + z_k(t) \\ z_k'(t) & = & az_k. \end{array}$$

The last equation implies

$$z_k(t) = c_k e^{at}$$

for some constant c_k. Consider

$$\frac{d}{dt}(z_{k-1}e^{-at}) = (z_{k-1}' - az_{k-1})e^{-at} = c_k.$$

Since this is a constant, we find

$$z_{k-1}(t) = (c_k t + c_{k-1})e^{at}.$$

We can now proceed by induction. Assume that we have shown that

$$z_i(t) = \left(\frac{c_k}{(k-i)!}t^{k-i} + \frac{c_{k-1}}{(i-k-1)!}t^{k-i-1} + \cdots + c_i\right)e^{at}.$$

Then

$$\frac{d}{dt}(z_{i-1}e^{-at}) = (z_{i-1}' - az_{i-1})e^{-at} = \frac{c_k}{(k-i)!}t^{k-i} + \frac{c_{k-1}}{(k-i-1)!}t^{k-i-1} + \cdots + c_i.$$

Hence, integrating both sides, we obtain

$$z_{i-1}(t) = \left(\frac{c_k}{(k-i+1)!}t^{k-i+1} + \frac{c_{k-1}}{(k-i)!}t^{k-i} + \cdots + c_{i-1}\right)e^{at}.$$

We can summarize:

PROPOSITION 3.38. *The solutions $z = (z_1, z_2, \ldots, z_k)$ to the system of differential equations*

$$z'(t) = J_k(a)z(t)$$

with a single Jordan block $J_k(a)$ are given by

$$z_i(t) = \left(\frac{c_k}{(k-i)!}t^{k-i} + \frac{c_{k-1}}{(i-k-1)!}t^{k-i-1} + \cdots + c_i\right)e^{at}$$

for $i = 1, \ldots, k$, where $c_1, \ldots, c_k$ are arbitrary constants.

EXAMPLE 3.39. We consider the system

$$\begin{aligned} y_1' &= y_2 \\ y_2' &= -y_1 - 2y. \end{aligned}$$

Here

$$A = \begin{bmatrix} 0 & 1 \\ -1 & -2 \end{bmatrix}.$$

The characteristic polynomial turns out to be

$$c_A(\lambda) = (\lambda + 1)^2.$$

The transformation $A+I$ is nilpotent of index 2 on $\mathbb{C}^2$ and $\{(1,-1),(1,0)\}$ is a Jordan basis of $\mathbb{C}^2$ that gives the Jordan canonical form for A:

$$J_2(-1) = \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}.$$

The matrix P that transforms A into the Jordan canonical form is given by

$$P = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix},$$

i.e.,

$$P^{-1}AP = J_2(-1).$$

The solutions $z(t) = (z_1(t), z_2(t))$ of the transformed system

$$\begin{aligned} z_1' &= -z_1 + z_2 \\ z_2' &= -z_2 \end{aligned}$$

are given by

$$\begin{aligned} z_1(t) &= (c_2 t + c_1)\, e^{-t} \\ z_2(t) &= c_2 e^{-t}. \end{aligned}$$

The solutions to the original system are then obtained via

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = P \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$$

as

$$\begin{aligned} y_1(t) &= (c_2 t + c_1 + c_2)\, e^{-t} \\ y_2(t) &= -(c_2 t + c_1)\, e^{-t}. \end{aligned}$$

CHAPTER 4

INNER PRODUCT SPACES

Throughout this section, V denotes a finite-dimensional vector space over the field F, where F is either the field $\mathbb{R}$ of real numbers or the field $\mathbb{C}$ of complex numbers. If

$$z = x + iy$$

is a complex number ($x, y \in \mathbb{R}$), then

$$\bar{z} = x - iy$$

denotes the complex conjugate of z. We note that

$$z = \bar{z} \iff z \in \mathbb{R}$$

and that

$$z\bar{z} = x^2 + y^2 = |z|^2.$$

DEFINITION 4.1. An **inner product** $\langle \cdot, \cdot \rangle$ is a map that assigns to any two vectors $u, v \in V$ a number $\langle u, v \rangle$ in F such that

1. $\langle u_1 + u_2, v \rangle = \langle u_1, v \rangle + \langle u_2, v \rangle$.
2. $\langle au, v \rangle = a\langle u, v \rangle$ for all $a \in F, u, v \in V$.
3. $\langle v, u \rangle = \overline{\langle u, v \rangle}$ for all $u, v \in V$.

Note that 3. implies that $\langle v, v \rangle \in \mathbb{R}$, and we want in addition:

4. $\langle v, v \rangle > 0$ for all $v \neq 0, v \in V$ (**positive definiteness**).

REMARK 4.2. Properties 1 and 2 show that the inner product is linear in the first variable, but we have

$$\langle u, av \rangle = \bar{a}\langle u, v \rangle$$

in the second variable, so it is not linear in this variable for general complex inner products. The vector space V, taken together with an inner product on it, is called an **inner product space**. Given $v \in V$, we define **the length of** v by

$$\|v\| = \sqrt{\langle v, v \rangle}.$$

Note that

$$\|av\| = |a|\|v\|$$

for all $a \in F, v \in V$. Furthermore, if $v \neq 0$, then $\frac{v}{\|v\|}$ has length 1.

Two vectors $u, v \in V$ are **orthogonal** if $\langle u, v \rangle = 0$. A basis $B = \{v_1, \ldots, v_n\}$ of V is an **orthonormal basis** (ONB) if all v_i have length 1 and if

$$\langle v_i, v_j \rangle = 0$$

for all $i \neq j$. If $B = \{v_1, \ldots, v_n\}$ is an ONB of V and

$$v = a_1 v_1 + \cdots + a_n v_n,$$

then it is easy to compute the coefficients a_i for $1 \leq i \leq n$:

$$a_i = \langle v, v_i \rangle,$$

so that

$$v = \langle v, v_1 \rangle v_1 + \cdots + \langle v, v_n \rangle v_n.$$

Moreover, if

$$w = b_1 v_1 + \cdots + b_n v_n$$

is any other vector from V, then

$$\langle v, w \rangle = a_1 \overline{b_1} + \cdots a_n \overline{b_n} = \langle v, v_1 \rangle \overline{\langle w, v_1 \rangle} + \cdots \langle v, v_n \rangle \overline{\langle w, v_n \rangle}.$$

The Gram-Schmidt process shows how to change any basis of a subspace W of V into an ONB for W. In particular, every inner product space has an ONB.

If W is a subspace of V, then the **orthogonal complement** $W^\perp$ of W is defined as

$$W^\perp = \{v \in V \mid \langle v, w \rangle = 0 \text{ for all } w \in W\}.$$

Note that $\langle v, w \rangle = 0 \iff \langle w, v \rangle = 0$, so we can also write

$$W^\perp = \{v \in V \mid \langle w, v \rangle = 0 \text{ for all } w \in W\}.$$

Clearly, $W^\perp$ is a subspace of V, and it is easy to see that

$$V = W \oplus W^\perp.$$

In particular,

$$\dim W + \dim W^\perp = \dim V.$$

Let $T \colon V \to V$ be a linear transformation. The problem we want to consider is that of giving necessary and sufficient conditions for T to be represented by a diagonal matrix with respect to some ONB. Let $B = \{v_1, \ldots, v_n\}$ be an arbitrary ONB, and let $A = A_T^B = (a_{ij})$ be the matrix representing T with respect to B so that

$$T(v_i) = A \cdot v_i$$

for $i = 1, \ldots, n$.

Definition 4.3. Let

$$\bar{A}^t = (\overline{a_{ji}})$$

denote the **conjugate transpose** of the matrix A. Let $T^* \colon V \to V$ be defined by

$$T^*(v_i) = \bar{A}^t \cdot v_i$$

for $i = 1, \ldots, n$, or in other words, so that $\bar{A}^t = A_{T^*}^B$. Then T^* is called the **adjoint** of T.

The following result characterizes the adjoint.

Proposition 4.4. *For all $u, v \in V$,*

$$\langle Tu, v \rangle = \langle u, T^* v \rangle.$$

Moreover, the adjoint T^* is uniquely determined by this property.

PROOF. It is enough to check this relation for the basis vectors. As before, let $A = (a_{ij})$. Then

$$Tv_i = \sum_{k=1}^{n} a_{ki} v_k,$$

and therefore

$$\langle Tv_i, v_j \rangle = a_{ji}.$$

On the other hand,

$$T^* v_j = \sum_{k=1}^{n} \overline{a_{jk}} v_k,$$

and therefore

$$\langle v_i, T^* v_j \rangle = \sum_{k=1}^{n} \langle v_i, \overline{a_{jk}} v_k \rangle = a_{ji},$$

as claimed.

If T' is another transformation satisfying

$$\langle Tu, v \rangle = \langle u, T'v \rangle$$

for all $u, v \in V$, then

$$\langle u, (T^* - T')v \rangle = 0$$

for all $u, v \in V$, so $T^* = T'$. □

We note the following easy properties:

1. $(T^*)^* = T$.
2. $(S + T)^* = S^* + T^*$.
3. $(aT)^* = \bar{a} T^*$.
4. $(ST)^* = T^* S^*$.

Assume now that V has an ONB B such that the matrix $A = A_T^B$ associated to T with respect to B is diagonal. Then

$$A = \operatorname{diag}(\lambda_1, \ldots, \lambda_n).$$

The matrix associated to T^* with respect to B then equals, by definition,

$$\bar{A}^t = \operatorname{diag}(\overline{\lambda_1}, \ldots, \overline{\lambda_n}).$$

It is clear that

$$A \cdot \bar{A}^t = \bar{A}^t \cdot A,$$

and therefore T and its adjoint T^* commute as well:

$$T \cdot T^* = T^* \cdot T.$$

If V is a *real* vector space, so that T has real eigenvalues, then we get a much stronger condition, namely that $A = \bar{A}^t$, and therefore in this case

$$T = T^*.$$

We summarize:

PROPOSITION 4.5. *Let $T\colon V \to V$ be a linear transformation on the inner product space V. If there exists an ONB B of V such that T is in diagonal form with respect to B, then $T \cdot T^* = T^* \cdot T$. Moreover, if V is real, then $T = T^*$.*

DEFINITION 4.6. A linear transformation $T\colon V \to V$ on an inner product space V is called **normal** if $TT^* = T^*T$ and **self-adjoint** if $T = T^*$. Note that the matrix of a real self-adjoint linear transformation with respect to an ONB is symmetric.

We want to show that the necessary conditions in Proposition 4.5 are also sufficient for the existence of an ONB that diagonalizes T. We need some facts about normal transformations, but first we prove a general result:

LEMMA 4.7. *Let W be a T-invariant subspace of the inner product space V. Then the orthogonal complement $W^\perp$ is T^*-invariant.*

PROOF. Let $v \in W^\perp$. We have to show that $T^*v \in W^\perp$, i.e., that $\langle w, T^*v\rangle = 0$ for all $w \in W$. Now,

$$\langle w, T^*v\rangle = \langle Tw, v\rangle.$$

Since W is T-invariant, we have $Tw \in W$, and hence

$$\langle Tw, v\rangle = 0,$$

v being in $W^\perp$. □

We now prove a few properties for normal transformations:

LEMMA 4.8. *If T is a normal transformation, then $\|Tv\| = \|T^*v\|$ for all $v \in V$.*

PROOF. We have

$$\|Tv\|^2 = \langle Tv, Tv\rangle = \langle v, T^*Tv\rangle = \langle v, TT^*v\rangle = \langle T^*v, T^*v\rangle = \|T^*v\|^2.$$

□

LEMMA 4.9. *Assume that $T\colon V \to V$ is normal. If λ is an eigenvalue of T, then $\bar\lambda$ is an eigenvalue of T^*, and the eigenspaces are the same.*

PROOF. We first note that the adjoint of $T-\lambda$ is equal to $T^*-\bar\lambda$. This immediately implies that $T - \lambda$ is again a normal transformation. Let v be an eigenvector for the eigenvalue λ of T. Applying Lemma 4.8 to the normal transformation $T - \lambda$ we obtain:

$$0 = \langle (T-\lambda)v, (T-\lambda)v\rangle = \langle (T^* - \bar\lambda)v, (T^* - \bar\lambda)v\rangle.$$

This implies that $(T^* - \bar\lambda)v = 0$, which was to be shown. □

LEMMA 4.10. *Assume that $T\colon V \to V$ is normal. Then eigenvectors belonging to different eigenvalues are orthogonal to each other.*

PROOF. Let λ_1 and λ_2 be different eigenvalues of T, and let v_1 and v_2 be eigenvectors belonging to λ_1 and λ_2, respectively. We have to show that $\langle v_1, v_2\rangle = 0$. Now

$$\lambda_1\langle v_1, v_2\rangle = \langle \lambda_1 v_1, v_2\rangle = \langle Tv_1, v_2\rangle = \langle v_1, T^*v_2\rangle = \langle v_1, \bar\lambda_2 v_2\rangle = \lambda_2\langle v_1, v_2\rangle.$$

Since $\lambda_1 \neq \lambda_2$, the result follows. □

We can now prove the first main result.

THEOREM 4.11. *Assume that $T\colon V \to V$ is a normal linear transformation, and assume that the minimal polynomial $m_T(x)$ of T splits into linear factors. Then there exists an ONB B for which the matrix of T with respect to B is diagonal.*

PROOF. We will prove the theorem by induction on the dimension of V, the result being clear if V is 1-dimensional. Since the minimal polynomial $m_T(x)$ of T splits, T has an eigenvalue λ. Let v_1 be an eigenvector for the eigenvalue λ. Since $v_1 \neq 0$, we can assume that $\|v_1\| = 1$. The 1-dimensional subspace $\langle v_1 \rangle$ of V is T-invariant since v_1 is an eigenvector. Hence, $Tv_1 = \lambda v_1$. By Lemma 4.9, v_1 is also an eigenvector of T^* for the eigenvalue $\overline{\lambda}$ of T^*. Hence, $T^*v_1 = \overline{\lambda}v_1$. This shows that the 1-dimensional cyclic subspace $\langle v_1 \rangle$ is also T^*-invariant. By Lemma 4.7, the orthogonal complement $\langle v_1 \rangle^\perp$ of $\langle v_1 \rangle$ is then T^{**}-invariant, hence T-invariant as $T^{**} = T$. We have therefore obtained a decomposition of V into an orthogonal sum of T-invariant subspaces,

$$V = \langle v_1 \rangle \oplus \langle v_1 \rangle^\perp,$$

which is also a decomposition of V into an orthogonal sum of T^*-invariant subspaces. Let $V_1 = \langle v_1 \rangle^\perp$, and let T_1 denote the restriction of T to V_1. Then T_1 is normal since the adjoint of T_1 is equal to the restriction of T^* to V_1. By induction, V_1 has an ONB B_1 for which the matrix of T_1 with respect to B_1 is diagonal. The basis $B = B_1 \cup \{v_1\}$ of V is then an ONB for V, and the matrix A_T^B representing T with respect to B is again diagonal. □

Since the minimal polynomial always splits into linear factors over the field $\mathbb{C}$ of complex numbers, we immediately obtain the following from Proposition 4.5 and Theorem 4.11.

COROLLARY 4.12. *Assume that V is a complex inner product space and that $T\colon V \to V$ is a linear transformation. Then T is normal if and only if there exists an ONB B of V for which T is in diagonal form.*

To obtain the analogous result in the real case, we only have to show that the minimal polynomial of a real self-adjoint linear transformation T splits into linear factors.

LEMMA 4.13. *Let V be a real vector space and $T\colon V \to V$ a self-adjoint linear transformation. Then the minimal polynomial $m_T(x)$ splits into linear factors.*

PROOF. Let A denote the matrix belonging to T with respect to some ONB of V. Then $A = A^t$. We can view A as a complex matrix. If λ is a complex eigenvalue of A with eigenvector v, then

$$\lambda v = Av = A^t v = \bar{\lambda} v,$$

so λ is in fact real. This implies that the minimal polynomial splits over $\mathbb{R}$. □

We obtain again from Proposition 4.5 and Theorem 4.11:

COROLLARY 4.14. *Assume that V is a real inner product space and that $T\colon V \to V$ is a linear transformation. Then T is self-adjoint if and only if there exists an ONB B of V for which T is in diagonal form with respect to B.*

A natural question now is to find out which linear transformations $U : V \to V$ map some ONB $B = \{v_1, \ldots, v_n\}$ to another ONB $B' = \{w_1, \ldots, w_n\}$. Assume that

$$U(v_i) = w_i \quad \text{for} \quad i = 1, \ldots, n.$$

The matrix A representing U with respect to the basis B is simply the base change matrix from B' to B:

$$A = (a_{ij}) = A_U^B = A_{B',B}.$$

For the coefficients a_{ij} of A, we have

$$a_{ij} = \langle w_j, v_i \rangle$$

since

$$w_j = \sum_{k=1}^{n} a_{kj} v_k.$$

The inverse matrix of A is simply the base change matrix from B to B' :

$$A^{-1} = (b_{ij}) = A_{B,B'},$$

and we have

$$b_{ji} = \langle v_i, w_j \rangle = \overline{\langle w_j, v_i \rangle} = \overline{a_{ij}}.$$

This shows that

$$A^{-1} = \overline{A}^t,$$

so

$$U^{-1} = U^* \quad \text{or} \quad UU^* = 1.$$

Definition 4.15. A linear transformation $U \colon V \to V$ is called **unitary** if V is complex and $UU^* = 1$ and **orthogonal** if V is real and $UU^* = 1$.

Here are some equivalent characterizations of unitary or orthogonal transformations:

Proposition 4.16. *Let V be an inner product space and $U \colon V \to V$ a linear transformation. The following are equivalent:*

1. *U is unitary or orthogonal.*
2. *$\langle Uv, Uw \rangle = \langle v, w \rangle$ for all $v, w \in V$.*
3. *U maps ONB's to ONB's.*

Proof. 1. $\Rightarrow$ 2. We have

$$\langle Uv, Uw \rangle = \langle v, U^*Uw \rangle = \langle v, w \rangle,$$

since $U^*U = 1$.

2. $\Rightarrow$ 3. Assume that $\{v_1, \ldots, v_n\}$ is an ONB. Then

$$\langle Uv_i, Uv_j \rangle = \langle v_i, v_j \rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

This shows that $\{Uv_1, \ldots, Uv_n\}$ is again an ONB.

3. $\Rightarrow$ 1. This direction was shown above as a motivation for the definition.

□

As a special case of property 2 above, we note that unitary or orthogonal linear transformations preserve the length of vectors:

$$\|Uv\| = \|v\|$$

for all $v \in V$. Conversely, if we assume that a linear transformation preserves the length of every vector, then it preserves all inner products. This can be seen as follows. We expand

$$\langle U(v+w), U(v+w)\rangle = \langle v+w, v+w\rangle$$

and obtain

$$\langle Uv, Uw\rangle + \langle Uw, Uv\rangle = \langle v, w\rangle + \langle w, v\rangle$$

for all $v, w \in V$. If V is a real inner product space, so that

$$\langle w, v\rangle = \langle v, w\rangle,$$

then this immediately implies that

$$\langle Uv, Uw\rangle = \langle v, w\rangle.$$

In the complex case, we argue as follows. Replacing v by iv, we obtain the equality:

$$i\langle Uv, Uw\rangle - i\langle Uw, Uv\rangle = i\langle v, w\rangle - i\langle w, v\rangle.$$

Hence, we have

$$\langle Uv, Uw\rangle - \langle Uw, Uv\rangle = \langle v, w\rangle - \langle w, v\rangle.$$

The result follows. We can state:

LEMMA 4.17. *U is unitary or orthogonal if and only if U preserves the length of all vectors in V.*

We note that a unitary transformation is necessarily normal. The following result characterizes the normal transformations that are unitary.

PROPOSITION 4.18. *A normal transformation T is unitary if and only if all eigenvalues λ of T have absolute value 1: $|\lambda| = 1$.*

PROOF. Let λ be an eigenvalue of T with eigenvector v. Then

$$\langle Tv, Tv\rangle = \langle \lambda v, \lambda v\rangle = \lambda\bar{\lambda}\langle v, v\rangle.$$

Hence, $\langle Tv, Tv\rangle = \langle v, v\rangle$ if and only if $\lambda\bar{\lambda} = |\lambda|^2 = 1$. Since V has an ONB consisting of eigenvectors by Corollary 4.12, the result follows from Lemma 4.17. □

Orthogonal transformations are not necessarily self-adjoint. In fact, they may not have eigenvalues at all. But if λ is an eigenvalue, then the same argument as in Proposition 4.18 shows that $\lambda = \pm 1$. We note this for future reference:

LEMMA 4.19. *The only possible eigenvalues for an orthogonal transformation are* ± 1.

THEOREM 4.20. *Let $U\colon V \to V$ be an orthogonal transformation. Then there exists an ONB B such that the matrix A_U^B representing U with respect to B is of the form*

$$A_U^B = \begin{bmatrix} D_1 & 0 & 0 & \cdots & 0 \\ 0 & D_2 & 0 & \cdots & 0 \\ 0 & 0 & A_3 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & A_m \end{bmatrix},$$

where $D_1 = I_s$, $D_2 = -I_t$ for some $s, t \geq 0$ and all A_i's are 2×2-matrices of the form

$$A_i = \begin{bmatrix} \cos\theta_i & \sin\theta_i \\ -\sin\theta_i & \cos\theta_i \end{bmatrix}.$$

PROOF. Let $T\colon V \to V$ denote the linear transformation $T = U + U^* = U + U^{-1}$. Clearly, T is self-adjoint, and according to Corollary 4.14 we can decompose V into an orthogonal sum of eigenspaces with respect to the eigenvalues λ_i of T,

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r,$$

where $V_i = n(T - \lambda_i) = E_{\lambda_i}$. Since U commutes with T, and therefore also with $T - \lambda_i$, the subspace V_i is U-invariant by Lemma 3.18. We can therefore restrict our attention to one of the subspaces V_i and hence assume that T has only one eigenvalue λ and that $V = E_\lambda$.

In this case, we have

$$T - \lambda = U + U^{-1} - \lambda = 0.$$

We multiply by U and obtain

$$U^2 - \lambda U + 1 = 0,$$

and therefore the minimal polynomial $m_U(x)$ divides $x^2 - \lambda x + 1$. Lemma 4.18 shows that the only possible eigenvalues of U are ± 1, and therefore $x \pm 1$ are the only possible linear factors dividing $x^2 - \lambda x + 1$. This happens precisely when $\lambda = \pm 2$. We obtain the following three possibilities:

$$\begin{array}{ll} \lambda = \ \ 2, & m_U(x) = x - 1 \\ \lambda = -2, & m_U(x) = x + 1 \\ \lambda \neq \pm 2, & m_U(x) = x^2 - \lambda x + 1 \text{ irreducible.} \end{array}$$

We note that in the first two cases the minimal polynomial is of degree 1, since it splits and therefore U is diagonalizable.

Let us look at the case that $m_U(x) = x^2 - \lambda x + 1$ is irreducible. Let v be any non-zero vector in V. Clearly v and Uv are linearly independent, since U has no eigenvectors. The subspace $\langle v \rangle = S(v, Uv)$ spanned by v and Uv is U-invariant, since

$$U^2 v = \lambda U v - v \in \langle v \rangle,$$

and it is also U^*-invariant, since $U^* = U^{-1}$ and

$$U^{-1} v = \lambda v - U v \in \langle v \rangle.$$

Lemma 4.7 implies that the subspace $\langle v\rangle^\perp$ is again U-invariant. Hence,

$$V = \langle v\rangle \oplus \langle v\rangle^\perp$$

is an orthogonal decomposition of V into U-invariant subspaces. This reduces the problem to the study of a single cyclic subspace $\langle v\rangle$ of dimension 2. We note that on a 2-dimensional space the minimal polynomial has the following interpretation.

$$m_U(x) = x^2 - \lambda x + 1 = x^2 - \operatorname{tr}(U)x + \det(U),$$

so that

$$\operatorname{tr} U = \lambda, \quad \det U = 1.$$

The following lemma then finishes the proof. □

LEMMA 4.21. *Let A be an orthogonal 2×2-matrix of determinant 1. Then A has the form*

$$A = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}.$$

PROOF. Let

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

Since A is orthogonal, we have

$$AA^t = A^tA = I,$$

which leads to the following equations:

$$a^2 + b^2 = 1, c^2 + d^2 = 1, ac + bd = 0, a^2 + c^2 = 1, b^2 + d^2 = 1, ab + cd = 0.$$

We obtain

$$a = \pm d, c = \mp b.$$

If $b = c \neq 0$, then $d = -a$, and therefore

$$\det A = ad - bc = -a^2 - b^2 = -1,$$

contradicting the fact that $\det A = 1$. We therefore must have $c = -b$, which implies that $d = a$.

Since $a^2 + b^2 = 1$, we can write $a = \cos\theta, b = \sin\theta$, and therefore

$$A = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix},$$

as claimed. □

CHAPTER 5

CODING THEORY

The basic idea behind coding theory is the following. Suppose we want to send a message that consists of a string of 0's and 1's. This message is divided into words of length k, i.e., we are sending k-tuples one after another. These words are elements of the vector space $\mathbb{F}_2^k$. During transmission, errors may occur in the original message, and we want to be able to detect and, if possible, correct these errors. In doing so, we embed $\mathbb{F}_2^k$ into a larger vector space $\mathbb{F}_2^n$, i.e., we send $n-k$ control digits, which hopefully will enable us to detect and correct at least some errors.

DEFINITION 5.1. A (n,k)**-code** $\mathcal{C}$ is a subset of $\mathbb{F}_2^n$ with 2^k elements. Any bijection

$$\mathbb{F}_2^k \to \mathcal{C}$$

is called an **encoding**. The quotient $\frac{k}{n}$ is called the **information rate** of the code $\mathcal{C}$.

We will consider elements of $\mathbb{F}_2^n$ as row vectors in this section. Let us consider some examples:

EXAMPLE 5.2. $n=4$, $k=2$, **Repetition Code**.
We take $\mathcal{C} = \{(a\,b\,a\,b) \in \mathbb{F}_2^4\}$ and encode

$$(a\,b) \mapsto (a\,b\,a\,b).$$

If one error occurs during transmission, then we can detect it, but not correct it. If, for example, $(b\,b\,a\,b)$ is received, then we know that an error must have occurred, but the original message might have been either $(a\,b\,a\,b)$ or $(b\,b\,b\,b)$.

EXAMPLE 5.3. $n=3$, $k=2$, **Parity Check Code**.
We take $\mathcal{C} = \{(a\,b\;\,a+b) \in \mathbb{F}_2^3\}$ and encode

$$(a\,b) \mapsto (a\,b\;\,a+b).$$

Since the sum of the digits in each code word is 0, we can again detect one error but not correct it. Note that the information rate is $\frac{2}{3}$ for this code, whereas it was $\frac{1}{2}$ in the first example.

EXAMPLE 5.4. $n=6$, $k=2$, **Repetition Code**.
We take $\mathcal{C} = \{(a\,b\,a\,b\,a\,b) \in \mathbb{F}_2^6\}$ and encode

$$(a\,b) \mapsto (a\,b\,a\,b\,a\,b).$$

This time, if only one error occurs, we still have two copies of the original message, and therefore we can correct 1 error. We can also detect two errors. If, e.g., we receive $(a\,a\,b\,b\,a\,b)$, then we know that at least two errors must have occurred.

Again, we can find a better code with higher information rate that has the same properties.

EXAMPLE 5.5. $n = 5$, $k = 2$.
We take $\mathcal{C} = \{(00000), (01101), (10011), (11110) \in \mathbb{F}_2^5\}$ and encode

$$(00) \mapsto (00000)$$
$$(01) \mapsto (01101)$$
$$(10) \mapsto (10011)$$
$$(11) \mapsto (11110).$$

This code has already some interesting features. Any two code words differ in at least 3 positions. Hence, if 1 error occurs, then there is a unique code word that differs from the received word in 1 position, and if 2 errors occur, then the received word is not a code word. Therefore, this code will again correct 1 error and detect 2 errors.

We will say that a code $\mathcal{C}$ is **r-error-detecting** (**r-error-correcting**) if it detects (resp., corrects) up to r errors. Example 5.5 gives a good code, since the code words are far apart in the vector space. We want to analyze this more generally.

DEFINITION 5.6. Given $x, y \in \mathbb{F}_2^n$, the **Hamming-distance** $d(x, y)$ between x and y is defined as the number of positions in which x and y differ.

LEMMA 5.7. *The Hamming-distance has the following properties:*

a. $d(x, y) \geq 0$, *and* $d(x, y) = 0 \iff x = y$.

b. $d(x, y) = d(y, x)$

c. $d(x, z) \leq d(x, y) + d(y, z)$.

PROOF. Only part c needs a little thought. If x and z differ in position i, then either x and y or y and z differ in position i, which proves the triangle inequality. □

Lemma 5.7 tells us that the Hamming-distance defines a *metric* on $\mathbb{F}_2^n$.

DEFINITION 5.8. The **closed ball** of radius r around x is defined as

$$B_r(x) = \{y \in \mathbb{F}_2^n \mid d(x, y) \leq r\}.$$

In order to measure how far apart code words are, we define:

DEFINITION 5.9. Let $\mathcal{C}$ be a (n, k)-code. Then

$$d = d(\mathcal{C}) = \min_{\substack{x \neq y \\ x,y \in \mathcal{C}}} d(x, y)$$

is called the **minimum distance** of $\mathcal{C}$, and $\mathcal{C}$ is then called an **(n, k, d)-code**.

In our first two examples, the minimum distance is 2. In the last two examples, it is 3. In order to formulate the first non-trivial result, we recall that, for any real number x, the **Gauss bracket** $[x]$ is defined as the largest integer $\leq x$.

THEOREM 5.10. *An (n, k, d)-code $\mathcal{C}$ can detect up to $d - 1$ errors and correct up to $[\frac{d-1}{2}]$ errors.*

PROOF. If up to $d-1$ errors occur during transmission, then the original code word is changed in at most $d-1$ positions. Since the minimal distance between code words is d, the received word is not a code word. Therefore, we know that errors have occurred.

Let $r = [\frac{d-1}{2}]$. Then

$$r = \begin{cases} \frac{d-1}{2} & \text{if } d \text{ is odd,} \\ \frac{d-2}{2} & \text{if } d \text{ is even.} \end{cases}$$

In any case, $2r+1 \leq d$. In order to show that $\mathcal{C}$ is r-error-correcting, we will show that the closed balls $B_r(x)$ of radius r around code words x are disjoint. The received message, which has $\leq r$ errors, will then lie in exactly one ball, and we recover the original word as the center of that ball.

Let x, z be different code words. Then, for any $y \in \mathbb{F}_2^n$, we have by Lemma 5.3 that

$$2r+1 \leq d \leq d(x,z) \leq d(x,y) + d(y,z),$$

hence either $d(x,y) \geq r+1$ or $d(y,z) \geq r+1$, which means that y cannot lie in both $B_r(x)$ and $B_r(z)$. □

With $r = [\frac{d-1}{2}]$ as above, we know that the balls $B_r(x)$ around different code words x are disjoint. Let us determine when these balls cover $\mathbb{F}_2^n$ completely.

LEMMA 5.11. *The ball $B_r(x)$ contains*

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{r}$$

elements.

PROOF. If $d(x,y) = i$, then x and y differ in exactly i positions. There are $\binom{n}{i}$ possibilities for choosing i positions out of n. Hence, there are exactly $\binom{n}{i}$ elements at distance i from x. Summing over $i = 0, 1, \ldots, r$ gives the result. □

Since we have 2^k distinct code words, the union of the disjoint balls $B_r(x)$ cover

$$2^k \left(\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{r} \right)$$

elements in $\mathbb{F}_2^n$. Since $\mathbb{F}_2^n$ contains 2^n vectors, we obtain:

PROPOSITION 5.12. *For an (n,k,d)-code $\mathcal{C}$, let $r = [\frac{d-1}{2}]$. Then*

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{r} \leq 2^{n-k}.$$

DEFINITION 5.13. An (n,k,d)-code $\mathcal{C}$ is called **optimal** if equality holds in Proposition 5.12, i.e., if the balls $B_r(x)$ around the code words cover the whole vector space $\mathbb{F}_2^n$.

Let us take for example $d(\mathcal{C}) = 3$, in which case $r = 1$. Then

$$\binom{n}{0} + \binom{n}{1} = 1 + n,$$

and the condition for an optimal code reads

$$1 + n = 2^{n-k}.$$

If we define $t = n - k$, then the condition is

$$n = 2^t - 1,\ k = n - t.$$

We will see below that, for each $t \geq 2$, there exists an optimal $(2^t-1, 2^t-1-t, 3)$-code. Note that in Example 5.5 we have a $(5, 2, 3)$-code, but

$$6 = 1 + 5 < 2^3 = 8,$$

hence this code is not optimal. Optimal codes with $d(\mathcal{C}) = 3$ have the information rate

$$1 - \frac{t}{2^t - 1},$$

which is very good for large t.

We now turn to linear codes:

DEFINITION 5.14. An (n, k)-code $\mathcal{C}$ is **linear** if $\mathcal{C}$ is a linear subspace of $\mathbb{F}_2^n$. If G is an $k \times n$-matrix G with rows that form a basis of $\mathcal{C}$, then G is called a **generator matrix** for $\mathcal{C}$.

If G is a generator matrix for $\mathcal{C}$, then encoding is very simple. The linear map

$$x \mapsto xG$$

from $\mathbb{F}_2^k$ to $\mathbb{F}_2^n$ is one-to-one.

Let us find generator matrices in Examples 5.2–5.5. We can take

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

$$G = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

respectively. Note that we have arranged the basis vectors so that G has the form

$$G = [I_k \mid A].$$

This is called the **standard form** of G, which we will assume from now on. It has the advantage that the first k digits of the encoded word are the original ones. Since G has rank k, the nullspace $n(G)$ of G has dimension $n - k$. Let $\{b_1, b_2, \ldots, b_{n-k}\}$ be a basis of $n(G)$. Then $Gb_i^t = 0$ for $i = 1, 2, \ldots, n-k$. Let H be the $(n-k) \times n$-matrix with rows $b_1, b_2, \ldots, b_{n-k}$. We obtain

$$GH^t = 0.$$

DEFINITION 5.15. The matrix H is called a **parity check matrix** for $\mathcal{C}$.

The reason for this name is the following. We have

$$(xG)H^t = 0$$

for all vectors $x \in \mathbb{F}_2^k$, and therefore

$$cH^t = 0$$

for all vectors $c \in \mathcal{C}$. Equivalently,

$$Hc^t = 0$$

for all code words c. Since H has rank $n-k$ and since $\mathcal{C}$ has dimension k, this shows that $\mathcal{C} = n(H)$. We therefore have:

PROPOSITION 5.16. *Let $\mathcal{C}$ be a linear (n,k)-code with generator matrix G and parity check matrix H. Then*

$$\mathcal{C} = \{xG \mid x \in \mathbb{F}_2^k\} = \{c \in \mathbb{F}_2^n \mid Hc^t = 0\}.$$

REMARK 5.17. Since we assume $G = [I_k \mid A]$ to be in standard form, we can take

$$H = [A^t \mid I_{n-k}].$$

To see this, note that

$$GH^t = I_k \cdot A + A \cdot I_{n-k} = 2A = 0$$

since the entries of A are in the field $\mathbb{F}_2$. In Example 5.5, we have

$$H = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

We have seen above that for general codes the error-detecting and correcting properties are reflected by the minimal distance. For linear codes, the minimal distance is easy to calculate from the parity check matrix. We start with a definition.

DEFINITION 5.18. Given $x \in \mathbb{F}_2^n$, we define its **weight** $w(x)$ to be the number of non-zero digits in x. In other words,

$$w(x) = d(x, 0).$$

LEMMA 5.19. *Let $\mathcal{C}$ be a linear code. Then*

$$d(\mathcal{C}) = \min_{\substack{x \neq 0 \\ x \in \mathcal{C}}} w(x).$$

PROOF. We have $w(x) = d(x,0)$ and $d(x,y) = w(x-y)$. Since $\mathcal{C}$ is linear, it contains $x - y$ for every $x, y \in \mathbb{C}$. □

We now have:

PROPOSITION 5.20. *Let $\mathcal{C}$ be a linear (n,k,d)-code with parity check matrix H. The minimal distance $d = d(\mathcal{C})$ is the maximal number d for which no $d-1$ columns of H are linearly dependent but some d columns are.*

PROOF. Let $c_1, c_2, \ldots, c_n$ denote the columns of H. Then for any $x \in \mathbb{F}_2^n$, $x = (x_1\, x_2\, \ldots\, x_n)$, we have that the column vector Hx^t is

$$x_1c_1 + x_2c_2 + \cdots + x_nc_n,$$

and

$$Hx^t = 0 \Longleftrightarrow x \in \mathcal{C}.$$

This shows that linear dependence relations between the columns arise only from code words. By Lemma 5.19, at least d digits in each code word are non-zero and exactly d digits are non-zero in some code word. Hence, the smallest dependence relation has to involve exactly d columns. □

COROLLARY 5.21. *We have $d(\mathcal{C}) = 3$ if and only if no two columns of H are the same but some three columns are dependent.*

COROLLARY 5.22. *We have $d - 1 \leq n - k$.*

PROOF. Since no $d-1$ columns of H are linearly dependent, the matrix H must have rank $\geq d - 1$. On the other hand, we know that H has rank $n - k$. □

As promised, we can now construct optimal linear codes of minimal distance 3. Let $t \geq 2$ be given. Let $n = 2^t - 1$ and $k = n - t$. The parity check matrix of such a linear code will be a $t \times n$-matrix, no 2 columns of which are the same. So we can take for the columns of H all the non-zero vectors in $\mathbb{F}_2^t$. This gives the desired code, called a **Hamming-code**.

EXAMPLES 5.23. a. $t = 2$, so $n = 3, k = 1$.
We have

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix},\ G = [1\,1\,1].$$

b. $t = 3$, so $n = 7, k = 4$.
We have

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

and

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

We note that optimal codes are very easy to decode. Every vector in $\mathbb{F}_2^n$ lies in exactly one ball of radius r around a code word, and we decode the vector by taking the center of the ball. Assume that we are in the situation of Example 5.23b, so $r = 1$, and that we receive a word

$$x = (0\,1\,1\,0\,0\,0\,1).$$

We can calculate

$$Hx^t = (0\,1\,0)^t.$$

On the other hand, the vector $(0\,1\,0)^t$ is the sixth column of H and therefore equal to He_6^t, where e_6 is the sixth standard basis vector of $\mathbb{F}_2^7$. Therefore $H(x - e_6)^t = 0$, so

$$x - e_6 = (0\,1\,1\,0\,0\,1\,1)$$

is a code word. Since $x - e_6$ is within radius 1 of x, we decode x into $(0\,1\,1\,0\,0\,1\,1)$.

APPENDIX A

THE RATIONAL CANONICAL FORM

Throughout, V denotes a finite-dimensional F-vector space and $T\colon V \to V$ is a linear transformation. The goal in this section is to show that there is a refinement of the decomposition of V into a direct sum of T-invariant subspaces discussed in Section 2. We first look at the "smallest" possible non-zero T-invariant subspaces. Let $v \in V, v \neq 0$. Any T-invariant subspace containing v has to contain all vectors $T^m v$ for $m = 1, 2, \ldots$. On the other hand, the subspace $\langle v \rangle$ of V generated by v and all vectors $T^m v$, $m = 1, 2, \ldots$ is already T-invariant and therefore contained in any other T-invariant subspace containing v.

DEFINITION A.1. Given $v \neq 0 \in V$, the T-invariant subspace $\langle v \rangle$ of V is called the **cyclic** subspace generated by v. Note that $\langle v \rangle$ depends on the given transformation T. If we want to emphazise this dependence, we call $\langle v \rangle$ **T-cyclic** or **cyclic relative** to T.

Since V is finite-dimensional, there exists $k \geq 1$ for which the vectors

$$v, Tv, T^2 v, \ldots, T^{k-1} v$$

are linearly independent, but $T^k v$ is dependent on $v, Tv, \ldots, T^{k-1} v$, so

$$T^k v = a_0 v + a_1 Tv + \cdots + a_{k-1} T^{k-1} v$$

for some $a_0, \ldots, a_{k-1} \in F$. The dimension of $\langle v \rangle$ is clearly equal to k and the set $B_v = \{v, Tv, \ldots, T^{k-1} v\}$ is an ordered basis for $\langle v \rangle$.

We can rewrite the relation for $T^k v$ as

$$(T^k - a_{k-1} T^{k-1} - \cdots - a_1 T - a_0) v = 0.$$

If we define

$$m_v(x) = x^k - a_{k-1} x^{k-1} - \cdots - a_1 x - a_0,$$

then we obtain $m_v(T)(v) = 0$, and clearly $m_v(x)$ is the monic polynomial of smallest degree with this property. We refer to $m_v(x)$ as the **order** of v or the **T-annihilator** of v. If $g(x)$ is any polynomial in $F[x]$ such that $g(T)v = 0$, then we can use the Euclidean algorithm and write

$$g(x) = Q(x) m_v(x) + R(x)$$

with $R(x) = 0$ or $\deg R(x) < \deg m_v(x)$. We obtain:

$$0 = g(T)v = Q(T) m_v(T) v + R(T) v = R(T) v,$$

and therefore $R(x) = 0$, because of the minimality of $m_v(x)$. This shows:

LEMMA A.2. *If $g(x) \in F[x]$ satisfies $g(T)v = 0$, then $m_v(x) \mid g(x)$.*

We obtain the following important result.

COROLLARY A.3. *For every non-zero vector v, the order $m_v(x)$ divides the minimal polynomial $m_T(x)$ of T:*

$$m_v(x) \mid m_T(x)$$

PROOF. The minimal polynomial has the property that $m_T(T) = 0$, so that in particular $m_T(T)v = 0$ for all vectors $v \in V$. The result follows from Lemma A.2. □

Let us consider the special case that the degree of $m_v(x)$ is equal to 1. This is equivalent to the fact that $Tv = \lambda v$ for some $\lambda \in F$, and $m_v(x) = x - \lambda$. In other words, the 1-dimensional cyclic subspaces $\langle v \rangle$ are precisely the subspaces generated by eigenvectors v of T:

LEMMA A.4. *The cyclic subspace $\langle v \rangle$ is 1-dimensional if and only if v is an eigenvector for T.*

In particular, we see that V has a basis of eigenvectors if and only if V can be decomposed into a direct sum of 1-dimensional cyclic subspaces.

Let T_v denote the restriction of T to the T-invariant cyclic subspace $\langle v \rangle$. The matrix $A_{B_v}^{T_v}$ describing T_v with respect to the basis $B_v = \{v, Tv, \ldots, T^{k-1}v\}$ of $\langle v \rangle$ is called the **companion matrix** of T_v. It is easy to calculate:

LEMMA A.5. *The companion matrix of T_v is equal to*

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{k-1} \end{bmatrix}$$

.

PROOF. For $1 \leq i \leq k-1$, the ith basis vector in B_v is mapped under T to the $(i+1)$th basis vector. The last basis vector $T^{k-1}v$ is mapped under T to

$$T^k v = a_0 v + \cdots + a_{k-1} T^{k-1} v,$$

which gives the result. □

There are three polynomials attached to T_v and the cyclic subspace $\langle v \rangle$: the order $m_v(x)$, the mimimal polynomial $m_{T_v}(x)$, and the characteristic polynomial $c_{T_v}(x)$ of T_v. They are related to each other as follows:

PROPOSITION A.6. *Let $\langle v \rangle$ be a cyclic subspace of V, and let T_v denote the restriction of T to $\langle v \rangle$. Then we have*

$$m_v(X) = m_{T_v}(x) = c_{T_v}(x).$$

PROOF. From Corollary A.3, we obtain $m_v(x) \mid m_{T_v}(x)$. By definition, $m_v(T)(v) = 0$. Since $m_v(T)$ commutes with any power of T, we have

$$m_v(T)(T^i v) = T^i m_v(T) v = 0.$$

Hence, $m_v(T) = 0$ on $\langle v \rangle$, which implies that $m_{T_v}(x) \mid m_v(x)$. Since both polynomials are monic, they are equal.

As before, let

$$m_v(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_1x - a_0,$$

and let $A = A^{T_v}_{B_v}$ denote the companion matrix. We have to calculate the determinant of

$$x \cdot I - A = \begin{bmatrix} x & 0 & \cdots & 0 & -a_0 \\ -1 & x & \cdots & 0 & -a_1 \\ 0 & -1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & x - a_{k-1} \end{bmatrix}$$

and show that it equals $x^k - a_{k-1}x^{k-1} - \cdots - a_1x - a_0$. We do this by induction on k. If $k = 1$, then the result is clear. Let us expand the matrix $x \cdot I - A$ along the first row. Then

$$\det(x \cdot I - A) = (x) \times \begin{vmatrix} x & 0 & \cdots & 0 & -a_1 \\ -1 & x & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & x - a_{k-1} \end{vmatrix} - a_0.$$

By induction, the determinant of the $(k-1) \times (k-1)$-matrix

$$\begin{bmatrix} x & 0 & \cdots & 0 & -a_1 \\ -1 & x & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & x - a_{k-1} \end{bmatrix}$$

is equal to

$$x^{k-1} - a_{k-1}x^{k-2} - \cdots - a_1.$$

Hence,

$$\begin{aligned} c_{T_v}(x) = \det(x \cdot I - A) &= x(x^{k-1} - a_{k-1}x^{k-2} - \cdots - a_1) - a_0 \\ &= x^k - a_{k-1}x^{k-1} - \cdots - a_1x - a_0, \end{aligned}$$

as claimed. □

In order to obtain the refined decomposition of V into a direct sum of cyclic subspaces, we can first use primary decomposition, Theorem 3.20, to reduce to the case that $m_T(x) = p(x)^e$ for some irreducible polynomial $p(x)$. Since the order $m_v(x)$ divides $m_T(x)$ for each non-zero $v \in V$, we have

$$m_v(x) = p(x)^{e_v}$$

for some $e_v \leq e$. Hence, the only possible orders are $p(x), p(x)^2, \ldots, p(x)^e$. Let $d = \deg p(x)$. Then the dimension of $\langle v \rangle$ is equal to

$$\dim \langle v \rangle = d \cdot e_v,$$

and therefore the only possible dimensions for a cyclic subspace $\langle v \rangle$, and therefore for the smallest T-invariant subspaces are $d, 2d, \ldots, ed$. We want to use a slightly

different basis for $\langle v\rangle$ than before. Let us rewrite the usual ordered basis as

$$\begin{array}{cccc} v, & Tv, & \dots, & T^{d-1}v, \\ T^d v, & T^{d+1}v & \dots, & T^{2d-1}v, \\ \vdots & \vdots & \vdots & \vdots \\ T^{d(e_v-1)}v & T^{d(e_v-1)+1}v & \dots & T^{de_v-1}v. \end{array}$$

Define $b_0, b_1, \dots b_{d-1}$ by

$$p(x) = x^d - b_{d-1}x^{d-1} - \cdots b_1 x - b_0.$$

For each i with $1 \le i \le e_v - 1$, we can replace the power $T^{di}v$ in the basis by $p(T)^i\, v$. In this way, we obtain a new ordered basis B'_v of the following form:

$$B'_v = \left\{ \begin{array}{cccc} v, & Tv, & \dots, & T^{d-1}v \\ p(T)v, & p(T)Tv & \dots, & p(T)T^{d-1}v \\ \vdots & \vdots & \vdots & \vdots \\ p(T)^{e_v-1}v & p(T)^{e_v-1}Tv & \dots & p(T)^{e_v-1}T^{d-1}v \end{array} \right\}.$$

Let us denote by C_v the subspace of $\langle v\rangle$ with basis $\{v, Tv, \dots, T^{d-1}v\}$. We note that C_v is *not* T-invariant if $e_v > 1$. The basis B'_v immediately produces a decomposition of $\langle v\rangle$ of the form

$$\langle v\rangle = C_v \oplus p(T)C_v \oplus \cdots \oplus p(T)^{e_v-1}C_v.$$

LEMMA A.7. *Assume that $m_v(x) = p(x)^{e_v}$ for some irreducible polynomial $p(x)$. Then, for $1 \le i \le e_v$, we have*

$$\langle v\rangle \cap n(p(T)^i) = p(T)^{e_v-i}\langle v\rangle.$$

PROOF. We have $p(T)^i p(T)^{e_v-i}\langle v\rangle = p(T)^{e_v}\langle v\rangle = 0$, and therefore

$$p(T)^{e_v-i}\langle v\rangle \subset \langle v\rangle \cap n(p(T)^i).$$

Assume now that $w \in \langle v\rangle \cap n(p(T)^i)$. Then we can write w in terms of the direct sum decomposition

$$\langle v\rangle = C_v \oplus p(T)C_v \oplus \cdots \oplus p(T)^{e_v-1}C_v$$

uniquely as

$$w = v_0 + p(T)v_1 + \cdots + p(T)^{e_v-1}v_{e_v-1},$$

where the v_j are vectors from C_v. Applying $p(T)^i$ and using the fact that $p(T)^i w = 0$ we obtain

$$0 = p(T)^i v_0 + \cdots + p(T)^{i+e_v-1}v_{e_v-1} = p(T)^i v_0 + \cdots + p(T)^{e_v-1}v_{e_v-i-1},$$

since $p(T)^{e_v} = 0$ on the subspace $\langle v\rangle$. Now

$$p(T)^i v_0 + \cdots + p(T)^{e_v-1}v_{e_v-i-1} \in p(T)^i C_v \oplus \cdots \oplus p(T)^{e_v-1}C_v,$$

and therefore each individual vector $p(T)^{i+j}v_j$ has to be zero. This shows that

$$w = p(T)^{e_v-i}v_{e_v-i} + \cdots + p(T)^{e_v-1}v_{e_v-1} = p(T)^{e_v-i}(v_{e_v-i} + \cdots + p(T)^{i-1}v_{e_v-1}),$$

as claimed. □

COROLLARY A.8. *Let $m_v(x) = p(x)^{e_v}$, let $w \in \langle v \rangle$, and let $m_w(x) = p(x)^{e_w}$. Then*

$$\langle w \rangle = p(T)^{e_v - e_w} \langle v \rangle.$$

PROOF. We have

$$w \in \langle v \rangle \cap n(p(T)^{e_w}),$$

so $w \in p(T)^{e_v - e_w} \langle v \rangle$ by Lemma A.7. Since $p(T)^{e_v - e_w} \langle v \rangle$ is T-invariant, it contains with w also the cyclic subspace $\langle w \rangle$:

$$\langle w \rangle \subset p(T)^{e_v - e_w} \langle v \rangle.$$

Both these subspaces of $\langle v \rangle$ have the same dimension $d \cdot e_w$, $d = \deg p(x)$. Hence, they are equal. □

The following result is crucial for the decomposition of a vector space into a direct sum of cyclic subspaces.

PROPOSITION A.9. *Assume that the minimal polynomial $m_T(x)$ for $T\colon V \to V$ equals $p(x)^e$. Let W be a T-invariant subspace of V. For each vector $v \in n(p(T))$ with $v \notin W$, we have*

$$W \cap \langle v \rangle = (0).$$

PROOF. Let $w \in W \cap \langle v \rangle$, and assume that $w \neq 0$. Since both W and $\langle v \rangle$ are T-invariant, so is their intersection. Thus,

$$\langle w \rangle \subset W \cap \langle v \rangle.$$

In particular, $\langle w \rangle \subset \langle v \rangle$. Now, we have $m_v(x) = p(x)$ since $v \in n(p(T))$. Hence, $m_w(x) = p(x)$ as well, since we are assuming that $w \neq 0$. Corollary A.8 implies now that $\langle w \rangle = \langle v \rangle$. Hence, $\langle v \rangle \subset W \cap \langle v \rangle$. In particular, $v \in W$, contradicting our assumption that $v \notin W$. Therefore, $w = 0$. □

Here are some consequences.

COROLLARY A.10. *Assume that $m_T(x) = p(x)^e$, and assume that W is a T-invariant subspace of V such that $n(p(T)) \not\subset W$. Then there exist $v_1, \ldots, v_s \in n(p(T))$ such that*

$$W + n(p(T)) = W \oplus \langle v_1 \rangle \oplus \langle v_2 \rangle \oplus \cdots \oplus \langle v_s \rangle.$$

PROOF. Since $n(p(T)) \not\subset W$, we find a non-zero vector $v_1 \in n(p(T)), v_1 \notin W$. Proposition A.9 implies that $W + \langle v_1 \rangle = W \oplus \langle v_1 \rangle$. If $W \oplus \langle v_1 \rangle = W + n(p(T))$, then we are done. Otherwise we find $v_2 \in n(p(T))$, $v_2 \notin W \oplus \langle v_1 \rangle$, and again Proposition A.9 shows that $W \oplus \langle v_1 \rangle + \langle v_2 \rangle = W \oplus \langle v_1 \rangle \oplus \langle v_2 \rangle$. We can proceed in this way until

$$W \oplus \langle v_1 \rangle \oplus \langle v_2 \rangle \oplus \cdots \oplus \langle v_s \rangle$$

contains $n(p(T))$, which means that

$$W + n(p(T)) = W \oplus \langle v_1 \rangle \oplus \langle v_2 \rangle \oplus \cdots \oplus \langle v_s \rangle.$$

□

We can now prove the first main result of this section:

THEOREM A.11. *Assume that the minimal polynomial $m_T(x)$ of $T\colon V \to V$ has the form $m_T(x) = p(x)^e$ for some irreducible polynomial $p(x) \in F[x]$. Then there exist vectors $v_1, v_2, \ldots, v_r \in V$ with*

$$V = \langle v_1 \rangle \oplus \langle v_2 \rangle \oplus \cdots \oplus \langle v_r \rangle.$$

The number r and the set of orders $\{m_{v_i}(x) = p(x)^{e_i}\}$ attached to $v_1, v_2, \ldots, v_r$ are uniquely determined by T.

PROOF. We proceed by induction on the power e in the minimal polynomial $m_T(x) = p(x)^e$. If $e = 1$, then $V = n(p(T))$, and taking $W = (0)$ in Corollary A.10, we obtain that

$$V = n(p(T)) = \langle v_1 \rangle \oplus \langle v_2 \rangle \oplus \cdots \oplus \langle v_r \rangle.$$

Each cyclic subspace $\langle v_i \rangle$ has order $m_{v_i}(x) = p(x)$ and is of dimension $d = \deg p(x)$. Therefore

$$\dim V = rd,$$

which determines r and the set of orders simply consists of r copies of $p(x)$.

Assume now that $e \geq 2$ and that the theorem is true for all linear transformations on finite-dimensional F-vector spaces for which the minimal polynomial has the form $p(x)^{e-1}$. We consider the linear map

$$p(T)\colon V \to V.$$

Let $\tilde{V}$ denote the range of $p(T)$,

$$\tilde{V} = p(T)\, V,$$

which is a T-invariant subspace of V. The restriction of T to $\tilde{V}$ has minimal polynomial $p(x)^{e-1}$. The induction hypothesis implies that

$$\tilde{V} = \langle w_1 \rangle \oplus \langle w_2 \rangle \oplus \cdots \oplus \langle w_s \rangle$$

and that s and the set of orders $m_{w_i}(x)$ are uniquely determined. We now choose vectors $v_1, \ldots, v_s$ in V such that

$$p(T)\, v_i = w_i \quad \text{for} \quad i = 1, \ldots, s.$$

Then clearly the order $m_{v_i}(x) = p(x)^{e_i}$ of v_i is equal to

$$m_{v_i}(x) = p(x) m_{w_i}(x).$$

In particular, all $e_i \geq 2$. Every basis vector $p(T)^j T^k v_i$ of $\langle v_i \rangle$ is mapped under $p(T)$ to $p(T)^j T^k w_i$, which implies that

$$p(T)\langle v_i \rangle = \langle w_i \rangle \quad \text{for} \quad i = 1, \ldots, s.$$

We now claim that, in fact, the sum of the cyclic subspaces $\langle v_i \rangle$ is again a direct sum:

$$\langle v_1 \rangle + \langle v_2 \rangle + \cdots + \langle v_s \rangle = \langle v_1 \rangle \oplus \langle v_2 \rangle \oplus \cdots \oplus \langle v_s \rangle.$$

To see this, let us assume that

$$0 = u_1 + \cdots + u_s$$

for some $u_i \in \langle v_i \rangle$. Applying $p(T)$, we obtain

$$0 = p(T)u_1 + \cdots + p(T)u_s.$$

But $p(T)u_i \in \langle w_i \rangle$, and the sum of the $\langle w_i \rangle$ is direct. Therefore,

$$p(T)u_i = 0 \quad \text{for} \quad i = 1, \ldots, s.$$

We obtain

$$u_i \in \langle v_i \rangle \cap n(p(T)) = p(T)^{e_i - 1}\langle v_i \rangle,$$

where we used Corollary A.8. We now note that $e_i \geq 2$, so

$$p(T)^{e_i - 1}\langle v_i \rangle \subset \langle w_i \rangle.$$

This shows that, for $1 \leq i \leq s$, the vector u_i is in fact in $\langle w_i \rangle$. But the sum of the $\langle w_i \rangle$'s is direct, so $u_i = 0$ for all i.

Let us define

$$W = \langle v_1 \rangle \oplus \cdots \oplus \langle v_s \rangle.$$

This is a T-invariant subspace of V. If $n(p(T)) \not\subset W$, then we can use Corollary A.10 to find additional cyclic subspaces $\langle v_{s+1} \rangle, \ldots, \langle v_r \rangle \in n(p(T))$ such that

$$W + n(p(T)) = \langle v_1 \rangle \oplus \langle v_2 \rangle \oplus \cdots \oplus \langle v_r \rangle.$$

We finally have to show that

$$V = W + n(p(T)).$$

This is an easy application of the dimension formula. First note that

$$\dim(W + n(p(T))) = \dim W + \dim n(p(T)) - \dim(W \cap n(p(T))).$$

Now $\dim W = \dim \tilde{V} + \dim(W \cap n(p(T)))$, and therefore

$$\dim(W + n(p(T))) = \dim \tilde{V} + \dim n(p(T)) = \dim V,$$

as claimed.

Let us assume that we have another decomposition of V into cyclic subspaces,

$$V = \langle v_1' \rangle \oplus \langle v_2' \rangle \oplus \cdots \oplus \langle v_q' \rangle.$$

Let us assume that the first t vectors v_i' have orders $p(x)^{e_i'}$ with $e_i' \geq 2$ and the remaining ones are in the nullspace of $p(T)$, and let

$$W' = \langle v_1' \rangle \oplus \langle v_2' \rangle \oplus \cdots \oplus \langle v_t' \rangle.$$

Applying $p(T)$, we obtain

$$\tilde{V} = p(T)\langle v_1' \rangle \oplus p(T)\langle v_2' \rangle \oplus \cdots \oplus p(T)\langle v_t' \rangle.$$

The induction hypothesis implies that $t = s$ and that the set orders of the vectors $p(T)v_i'$ is the same as the set of orders of the w_i. Hence, the set of orders for the v_i' is the same as that of the v_i's. But this shows that $\dim W' = \dim W$ and hence $q = r$, which finishes the proof. □

Here is a list of important consequences of Theorem A.11:

COROLLARY A.12. *Let $T\colon V \to V$ be a linear transformation with minimal polynomial $m_T(x) = p(x)^e$ and characteristic polynomial $c_T(x)$. Let $d = \deg p(x)$.*

a. $m_T(x) \mid c_T(x)$.

b. $c_T(T) = 0$ (Cayley-Hamilton Theorem).

c. $c_T(x) = p(x)^n$ with $n \cdot d = \dim V$.

d. If $V = \langle v_1\rangle \oplus \langle v_2\rangle \oplus \cdots \oplus \langle v_r\rangle$ *and* $m_{v_i} = p(x)^{e_i}$ *for* $i = 1, \ldots, r$, *then*

$$e = \max\{e_1, e_2, \ldots, e_r\}.$$

e. The number r *of cyclic subspaces is related to the dimension of the nullspace of* $p(T)$ *by*

$$d \cdot r = \dim n(p(T)).$$

Proof. Let

$$V = \langle v_1\rangle \oplus \langle v_2\rangle \oplus \cdots \oplus \langle v_r\rangle$$

be a decomposition of V into a direct sum of cyclic subspaces, and let T_i denote the restriction of T to $\langle v_i\rangle$. By Lemma 3.17,

$$c_T(x) = c_{T_1}(x) \cdots c_{T_r}(x).$$

Moreover, by Proposition A.6,

$$c_{T_i}(x) = m_{T_i}(x) = m_{v_i}(x).$$

Since $m_{v_i}(x)$ is equal to $p(x)^{e_i}$, we obtain a, b, and c. Since

$$m_T(x) = p(x)^e = \operatorname{lcm}(m_{T_1}(x), \ldots, m_{T_r}(x)) = p(x)^{\max\{e_1, e_2, \ldots, e_r\}},$$

there has to be at least one vector v_i for which $m_{v_i}(x) = p(x)^e$, which proves part d.

We have, by Lemma A.7,

$$n(p(T)) = n(p(T)) \cap \langle v_1\rangle \oplus \cdots \oplus\ n(p(T)) \cap \langle v_r\rangle =$$
$$= p(T)^{e_1 - 1}\langle v_1\rangle \oplus \cdots \oplus p(T)^{e_r - 1}\langle v_r\rangle.$$

Now $\deg p(x) = d$. Hence, each summand on the right-hand side has dimension d. Therefore,

$$\dim n(p(T)) = d \cdot r,$$

which proves e. □

Because of primary decomposition, Theorem 3.20, we immediately obtain from Theorem A.11 the following general result which works for arbitrary linear transformations on finite-dimensional F-vector spaces.

Theorem A.13 (Divisor Theorem). *Let* $T\colon V \to V$ *be a linear transformation on a finite-dimensional* F*-vector space. Assume that the minimal polynomial* $m_T(x)$ *factors as*

$$m_T(x) = p_1(x)^{e_1} p_2(x)^{e_2} \cdots p(x)^{e_r}$$

with distinct monic irreducible polynomials $p_1(x), \ldots, p_r(x)$. *Then there exist vectors* $v_1, \ldots v_m \in V$ *such that*

$$V = \langle v_1\rangle \oplus \cdots \oplus \langle v_m\rangle,$$

and for each i *the order* $m_{v_i}(x)$ *of* v_i *is equal to the power of some irreducible polynomial* $p_j(x)$ *dividing* $m_T(x)$. *The number* m *of cyclic subspaces and the set of orders* $\{m_{v_1}(x), \ldots, m_{v_m}(x)\}$ *are uniquely determined by* T.

Definition A.14. The set of orders $\{m_{v_1}(x), \ldots, m_{v_m}(x)\}$ is called the set of **elementary divisors** of T. The elementary divisors are uniquely determined by T, they are all powers of an irreducible polynomial, and they may well occur more than once.

Corollary A.12 generalizes to:

COROLLARY A.15. *Let $T\colon V \to V$ be a linear transformation on a finite-dimensional F-vector space. Then*

a. $m_T(x) \mid c_T(x)$. In particular, $c_T(T) = 0$ (Cayley-Hamilton).

b. $m_T(x)$ and $c_T(x)$ have the same prime divisors.

The decomposition of V into cyclic subspaces yields a nice matrix representation for T, provided we choose a suitable basis for a cyclic subspace $\langle v\rangle$. At the beginning of this chapter, we chose a basis B'_v of $\langle v\rangle$. In order to obtain an upper triangular matrix in case that the order $m_v(x)$ is linear, we rearrange the basis vectors in B'_v in the following way, and we denote the new basis by $\tilde{B}_v$. Note that $m_v(x) = p(x)^e$ and $\deg p(x) = d$.

$$\tilde{B}_v = \left\{ \begin{array}{cccc} p(T)^{e_v-1}v & p(T)^{e_v-1}Tv & \dots & p(T)^{e_v-1}T^{d-1}v \\ p(T)^{e_v-2}v & p(T)^{e_v-2}Tv & \dots & p(T)^{e_v-2}T^{d-1}v \\ \vdots & \vdots & \vdots & \vdots \\ p(T)v, & p(T)Tv & \dots, & p(T)T^{d-1}v \\ v, & Tv, & \dots, & T^{d-1}v \end{array} \right\}.$$

The calculation of the matrix representing T on $\langle v\rangle$ with respect to this basis is easy once we know how to express

$$p(T)^iT^dv = T(p(T)^iT^{d-1}v)$$

in terms of the basis vectors. We write

$$p(T) = T^d - b_{d-1}T^{d-1} - \cdots - b_1T - b_0,$$

so

$$T^d = p(T) + b_{d-1}T^{d-1} + \cdots + b_1T + b_0.$$

We obtain

$$p(T)^iT^dv = p(T)^{i+1}v + b_{d-1}p(T)^iT^{d-1}v + \cdots + b_1p(T)^iTv + b_0p(T)^iv.$$

If we define the following $d \times d$-matrices,

$$A = \begin{bmatrix} 0 & 0 & \cdots & 0 & b_0 \\ 1 & 0 & \cdots & 0 & b_1 \\ 0 & 1 & \cdots & 0 & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & b_{d-1} \end{bmatrix}$$

and

$$B = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix},$$

then the $d \cdot e \times d \cdot e$-matrix representing T with respect to the basis $\tilde{B}_v$ is of the form

$$\begin{bmatrix} A & B & 0 & \cdots & 0 \\ 0 & A & B & \ddots & \vdots \\ 0 & 0 & A & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & B \\ 0 & \cdots & 0 & 0 & A \end{bmatrix}.$$

If we take these bases on each cyclic direct summand in a decomposition of V, then the associated matrix is called **rational canonical form**.

EXAMPLE A.16. Assume that the elementary divisors of a linear transformation $T\colon V \to V$, where V is a real vector space, are given by

$$\{x-1, (x-1)^2, x^2+1, (x^2+1)^3\}.$$

Then we know that

$$V = \langle v_1 \rangle \oplus \langle v_2 \rangle \oplus \langle v_3 \rangle \oplus \langle v_4 \rangle,$$

where

$$\begin{aligned} m_{v_1}(x) &= x-1, \\ m_{v_2}(x) &= (x-1)^2, \\ m_{v_3}(x) &= x^2+1, \\ m_{v_4}(x) &= (x^2+1)^3. \end{aligned}$$

Hence, the dimensions of the cyclic subspaces $\langle v_i \rangle$ are given respectively by $1, 2, 2, 6$, and V is 11-dimensional. The characteristic polynomial of T is equal to the product of the elementary divisors, so

$$f_T(x) = (x-1)^3(x^2+1)^4.$$

The minimal polynomial of T is the lcm of the elementary divisors, so

$$m_T(x) = (x-1)^2(x^2+1)^3.$$

With respect to the ordered basis

$$\{v_1, (T-1)v_2, v_2, v_3, Tv_3, (T^2+1)v_4, (T^2+1)Tv_4, v_4, Tv_4\}$$

the rational canonical form of T is equal to

$$\left[\begin{array}{c:cc:cc:cccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hdashline
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hdashline
0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hdashline
0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{array}\right]$$

The general problem is to find the elementary divisors and generators for the corresponding cyclic subspaces. We illustrate this in the following examples.

EXAMPLES A.17. a. Let $T\colon \mathbb{R}^5 \to \mathbb{R}^5$ be given by the matrix

$$A = \begin{bmatrix} -1 & 2 & -2 & 2 & 0 \\ -1 & 1 & -1 & 2 & 0 \\ 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & -1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

The characteristic polynomial $c_T(x)$ is equal to

$$c_T(x) = (x-1)(x^2+1)^2,$$

so we know that $m_T(x) = (x-1)(x^2+1)$ or $m_T(x) = (x-1)(x^2+1)^2$.

The matrix representing T^2+1 is equal to

$$A^2 + I = \begin{bmatrix} 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix},$$

which has rank 1. Thus,

$$\dim n(T^2+1) = 4 = 2 \cdot 2.$$

This shows that

$$m_T(x) = (x-1)(x^2+1).$$

Without calculating a basis, we know already that

$$\mathbb{R}^5 = \langle v_1 \rangle \oplus \langle v_2 \rangle \oplus \langle v_3 \rangle,$$

where v_1 is an eigenvector for the eigenvalue 1 and v_2 and v_3 are in the nullspace of $T^2 + 1$. The cyclic subspace $\langle v_1 \rangle$ is 1-dimensional, and the cyclic subspaces v_2 and v_3 are each two-dimensional with bases v_2, Tv_2 and v_3, Tv_3, respectively. Then the canonical form for T with respect to the ordered basis $\{v_1, v_2, Tv_2, v_3, Tv_3\}$ equals

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

How do we find the basis vectors v_i? We know that

$$\mathbb{R}^5 = n(T - 1) \oplus n(T^2 + 1).$$

The nullspace of $T-1$ is 1-dimensional generated by $v_1 = (1, 1, 1, 1, 1)$. The calculation above for $A^2 + 1$ shows that $n(T^2 + 1)$ has basis e_1, e_2, e_3, e_4. Let us take

$$v_2 = e_1 = (1, 0, 0, 0, 0).$$

Then

$$T(v_2) = Av_2 = (-1, -1, 0, 0, 0).$$

The cyclic subspace $\langle v_2 \rangle$ does not contain e_3 (or e_4), so we can take $v_3 = e_3$. Then

$$Te_3 = (-2, -1, -1, -1, 0),$$

and we are done.

b. Let us consider a slightly different example. This time we take A to be

$$A = \begin{bmatrix} 0 & 1 & -2 & 2 & 0 \\ 0 & 0 & -1 & 2 & 0 \\ 1 & -1 & -1 & 2 & 0 \\ 1 & -1 & -1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Again, the characteristic polynomial is equal to

$$c_T(x) = (x - 1)(x^2 + 1)^2.$$

We calculate

$$A^2 + I = \begin{bmatrix} 1 & 0 & -1 & 0 & 2 \\ 1 & 0 & -1 & 0 & 2 \\ 1 & 0 & -1 & 0 & 2 \\ 0 & 1 & -1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix}.$$

The rank of this matrix is equal to 3 and therefore

$$\dim n(T^2 + 1) = 2,$$

which implies that

$$m_T(x) = (x - 1)(x^2 + 1)^2$$

and that

$$\mathbb{R}^5 = \langle v_1 \rangle \oplus \langle v_2 \rangle,$$

where v_1 is an eigenvector for the eigenvalue 1 and $\langle v_2 \rangle$ is a cyclic subspace of dimension 4 with ordered basis

$$\{(T^2+1)v_2, (T^2+1)Tv_2, v_2, Tv_2\}.$$

With respect to the ordered basis

$$\{v_1, (T^2+1)v_2, (T^2+1)Tv_2, v_2, Tv_2\},$$

we obtain the rational canonical form

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Again, the eigenspace for the eigenvalue 1 is 1-dimensional, generated by $v_1 = (1,1,1,1,1)$. For v_2, we can take any non-zero vector in the nullspace of $(T^2+1)^2$ that is not in the nullspace of T^2+1. Since

$$(A^2+I)^2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 4 \end{bmatrix},$$

we see that e_1, e_2, e_3, e_4 is a basis for $n((T^2+1)^2)$. We can take $v_2 = e_1$. Then

$$\begin{aligned} Te_1 = Ae_1 &= (0,0,1,1,0), \\ (T^2+1)e_1 &= (1,1,1,0,0), \\ (T^2+1)^2Te_1 &= (1,-1,-1,-1,0) \end{aligned}$$

so that the ordered basis for $\mathbb{R}^5$ is equal to

$$\{(1,1,1,1,1), (1,1,1,0,0), (1,-1,-1,-1,0), (1,0,0,0,0), (0,0,1,1,0)\}.$$

It may happen that all the irreducible polynomials dividing $m_T(x)$ (or $c_T(x)$) are linear: e.g., if V is a vector space over the field $\mathbb{C}$ of complex numbers. In this case,

$$m_T(x) = (x-\lambda_1)^{e_1}(x-\lambda_2)^{e_2}\cdots(x-\lambda_r)^{e_r},$$

where the λ_i are the distinct eigenvalues of T. The rational canonical form is then called *Jordan canonical form* or *Jordan normal form*. It takes a very simple form. Let $\langle v \rangle$ be a cyclic subspace with order $m_v(x) = (x-\lambda)^e$. The basis $\tilde{B}_v$ looks like

$$\tilde{B}_v = \{(T-\lambda)^{e-1}v, (T-\lambda)^{e-2}v, \ldots, (T-\lambda)v, v\},$$

and the matrix is given by a *Jordan block of size* $e \times e$:

$$\begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{bmatrix}.$$

For examples of the Jordan canonical form, see Section 3.