Lineare Algebra I

Prof. Dr. Peter Müller

Inhaltsverzeichnis

1 Sprache der Mathematik

1.1 Definition / Bemerkung

Wir werden Mengen nicht formal definieren, sondern betrachten sie als eine Ansammlung von Objekten, den Elementen. Gehört ein Element x zur Menge M, so schreibt man $x \in M$, ansonsten $x \notin M$.

1.2 Bemerkung

1. Leere Menge $M = \{\ \} = \emptyset$
2. Natürliche Zahlen $\mathbb{N} = \{0,\ 1,\ 2,\ \ldots\}$
3. Ganze Zahlen $\mathbb{Z} = \{0,\ \pm 1,\ \pm 2,\ \ldots\}$

Mengen werden oft in der Form $M = \{n \mid \text{für } n \text{ gilt} \ldots\}$ beschrieben, etwa $P = \{2, 3, 5, 7, 11, \ldots\} = \{p \in \mathbb{N} \mid p \text{ ist prim}\}$.

Seien nun A, B Mengen. Gilt dann $a \in B$ für alle $a \in A$, so schreibt man $A \subseteq B$. Gibt es ein $b \in B$ mit $b \notin A$, so schreibt man $A \subsetneq B$.

1.3 Definition

1. $A \cap B = \{x \mid x \in A \wedge x \in B\}$
2. $A \cup B = \{x \mid x \in A \vee x \in B\}$
3. $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$

Sei $n \in \mathbb{N}$ und $n \geq 1$. Das karthesische Produkt $M_1 \times \ldots \times M_n$ der Mengen $M_1, \ldots, M_n$ ist die Menge der Tupel $(m_1,\ \ldots,\ m_n)$ mit $m_1 \in M_n,\ \ldots,\ m_n \in M_n$. Ein Spezialfall ist $M_1 = \ldots = M_n$, dann schreibt man auch M^n.

1.4 Definition

Seien A, B Mengen. Eine Relation R ist eine Teilmenge $R \subseteq A \times B$ des karthesischen Produkts von A und B. Man schreibt dann auch $a \sim b$, falls $(a,\ b) \in R$.

Sei $A = B$ und R eine Relation auf A. Die Relation R heißt:

1. reflexiv, falls $a \sim a$ für alle $a \in A$

2. symmetrisch, falls $a \sim b \Rightarrow b \sim a$ für alle $a,\ b \in A$

3. antisymmetrisch, falls $a \sim b \wedge b \sim a \Rightarrow a = b$ für alle $a,\ b \in A$

4. transitiv, falls $a \sim b \wedge b \sim c \Rightarrow a \sim c$ für alle $a,\ b,\ c \in A$

1.5 Bemerkung

Reflexivität ist eine Tatsache, die für alle $a \in A$ gelten muss. Symmetrie, Antisymmetrie und Transitivität sind dagegen Aussagen, die auch wahr sind, wenn ihre Voraussetzung falsch ist – etwa wenn $(a, b) \notin R$.

1.6 Definition

Eine reflexive, symmetrische und transitive Relation heißt Äquivalenzrelation. Für $x \in A$ nennt man dann $[x] = \{y \in A \mid y \sim x\}$ die Äquivalenzklasse von x.

1.7 Lemma

Für eine Äquivalenzrelation sind folgende Aussagen äquivalent:

1. $[x] \cap [y] \neq \emptyset$

2. $x \sim y$

3. $[x] = [y]$

Beweis

Zunächst sieht man $[x] \neq \emptyset$ für jede Äquivalenzklasse einer Äquivalenzrelation R, denn R reflexiv $\Rightarrow x \sim x \Rightarrow x \in [x]$.

[$1 \Rightarrow 2$] Sei $a \in [x] \cap [y]$. Dann gilt $a \sim x$, d.h. wegen der Symmetrie $x \sim a$, und $a \sim y$. Aus der Transitivität folgt dann $x \sim y$.

[$2 \Rightarrow 3$] Sei $a \in [x]$ beliebig. Dann gilt $a \sim x$ und $x \sim y$, also $a \sim y$ bzw. $a \in [y]$. Da dies für alle $a \in [x]$ gilt, ist $[x] \subseteq [y]$. Analog folgt $[y] \subseteq [x]$, also $[x] = [y]$.

[$3 \Rightarrow 1$] Es gilt $[x] \cap [y] = [x]$ mit $[x] \neq \emptyset$.

1.8 Korollar

Die Äquivalenzklassen einer Äquivalenzrelation auf A bilden eine disjunkte Zerlegung von A.

Beweis

Zu jedem $x,\, y \in A$ gibt es eine Äquivalenzklasse. Für diese gilt dann nach Lemma 1.7 entweder $[x] = [y]$ oder $[x] \cap [y] \neq \emptyset$.

1.9 Definition

Seien M, N Mengen. Eine Abbildung $f : M \longrightarrow N$ ordnet jedem $m \in M$ ein $f(m) \in N$ zu.

Genauer ist eine Abbildung $M \longrightarrow N$ eine Relation $R \subseteq M \times N$, für die gilt: $(m,\, n_1),\, (m,\, n_2) \in R \Rightarrow n_1 = n_2$ und $\forall_{m \in M}\, \exists_{n \in N}\, (m,\, n) \in R$.

Die Abbildung $f : M \longrightarrow N$ heißt injektiv, falls $m_1 \neq m_2 \Rightarrow f(m_1) \neq f(m_2)$ bzw. $f(m_1) = f(m_2) \Rightarrow m_1 = m_2$. Sie heißt surjektiv, falls $f(M) = \{f(m) \mid m \in M\} = N$, d.h. $\forall_{n \in N}\, \exists_{m \in M}\, f(m) = n$. f heißt bijektiv, falls f injektiv und surjektiv ist.

1.10 Definition

Ist M eine endliche Menge, dann bedeutet $|M|$ die Anzahl der Elemente. Ist M unendlich, so schreibt man $|M| = \infty$. Sind M und N Mengen, so setzt man $|M| = |N|$, falls es eine Bijektion zwischen M und N gibt.

Beispiel

1. $|\mathbb{Z}| = |2\mathbb{Z}|$ mit $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$, da $f : k \in \mathbb{Z} \longmapsto 2k \in 2\mathbb{Z}$ bijektiv ist.

2. Es gilt etwa $|\mathbb{Z}| = \infty$ und auch $|\mathbb{R}| = \infty$, aber dennoch $|\mathbb{Z}| \neq |\mathbb{R}|$.

1.11 Definition

In einem indirekten Beweis führt man das Gegenteil der zu beweisenden Aussage zu einem Widerspruch.

Beispiel

$\sqrt{2}$ ist irrational.

Indirekter Beweis

Wir nehmen an, $\sqrt{2}$ sei rational und führen diese Annahme auf einen Widerspruch.

Es folgt $0 < \sqrt{2} \in \mathbb{Q} \Rightarrow \sqrt{2} = \frac{m}{n}$ mit $m, n \in \mathbb{N} \setminus \{0\}$ teilerfremd. Also ist $2n^2 = m^2$, d.h. 2 ist ein Teiler von m^2. Da 2 eine Primzahl ist, ist 2 ein Teiler von m, d.h. $m = 2l$ für ein $l \in \mathbb{N} \setminus \{0\}$. Somit ist $2n^2 = 4l^2$, also $n^2 = 2l^2$. Analog ist dann 2 auch ein Teiler von n - ein Widerspruch zur teilerfremden Wahl von m und n.

1.12 Definition

Durch vollständige Induktion beweist man Aussagen $A(n)$, die von $n \in \mathbb{N}$ abhängen. Dann zeigt man:

1. $A(1)$ ist wahr.
2. Ist $A(n)$ für ein beliebiges $n \in \mathbb{N}$ wahr, so auch $A(n+1)$.

Dann sieht man nacheinander, dass $A(1)$, $A(2)$, ... wahr sind. Dabei heißt 1 die Induktionsverankerung und 2 der Induktionsschritt mit der Induktionsannahme, dass $A(n)$ wahr ist.

Beispiel

Es gilt $\sum\limits_{k=1}^{n}(2k-1) = n^2$ für alle $n \in \mathbb{N}$.

Beweis durch vollständige Induktion

Die Ausssage ist richtig für $n = 1$, da $\sum\limits_{k=1}^{1}(2k-1) = 1 = 1^2$.

Sei die Aussage nun richtig für n. Dann ist auch $\sum\limits_{k=1}^{n+1}(2k-1) = \sum\limits_{k=1}^{n}(2k-1) + (2(n+1)-1) = n^2 + 2n + 1 = (n+1)^2$.

1.13 Bemerkung

Zwei Varianten der vollständigen Induktion betriffen Aussagen $A(p)$ mit $p \in \mathbb{Z}$ und $p \geq q$ für ein festes $q \in \mathbb{Z}$. Dann zeige man:

1. $A(q)$ ist wahr.
2. Ist $A(p)$ für ein beliebiges $p \geq q$ wahr, dann auch $A(p+1)$.

oder man zeige:

1. $A(q)$ ist wahr.
2. Gilt $A(k)$ für alle $a \leq k \leq p$ mit beliebigem $p \geq q$, so auch $A(p+1)$.

Beispiel (Fibonacci-Zahlen)

Die Folge f_0, f_1, ... ist definiert durch

$$\begin{aligned} f_0 &= 0 \\ f_1 &= 1 \\ f_{n+1} &= f_n + f_{n-1} \text{ für } n \geq 1. \end{aligned}$$

Sei nun $\alpha = \frac{\sqrt{5}+1}{2}$. Dann gilt $f_n = \frac{\alpha^n - (1-\alpha)^n}{\sqrt{5}}$ für alle $n \in \mathbb{N}$.

Beweis

Die Behauptung stimmt offenbar für $n = 0$. Es sei nun $n \geq 0$ und für $0 \leq k \leq n$ gelte $f_k = \frac{\alpha^k - (1-\alpha)^k}{\sqrt{5}}$. Für $n \geq 1$ benutzen wir das Bildungsgesetz $f_{n+1} = f_n + f_{n-1}$ und die Induktionsannahme, d.h. die Induktion muss zusätzlich in $n = 1$ verankert werden: $f_1 = \frac{\alpha - (1-\alpha)}{\sqrt{5}} = 1$.

Man erhält

$$\begin{aligned} f_{n+1} &= f_n + f_{n-1} \\ &= \frac{\alpha^n - (1-\alpha)^n}{\sqrt{5}} + \frac{\alpha^{n-1} - (1-\alpha)^{n-1}}{\sqrt{5}} \\ &= \frac{\alpha^n + \alpha^{n-1} - (1-\alpha)^n - (1-\alpha)^{n-1}}{\sqrt{5}} \\ &= \frac{\alpha^{n-1} \cdot (\alpha+1) - (1-\alpha)^{n-1} \cdot (2-\alpha)}{\sqrt{5}} \end{aligned}$$

und wegen $1 + \alpha = \alpha^2$ sowie $2 - \alpha = (1-\alpha)^2$ folgt die Behauptung.

1.14 Bemerkung

Bei Induktionsbeweisen muss man sehr vorsichtig sein. Eine häufige Fehlerquelle ist dabei die Ungültigkeit des Induktionsschrittes für ein $n \in \mathbb{N}$.

Beispiel

Alle Menschen haben die gleiche Haarfarbe.

„Beweis“

Wir zeigen durch vollständige Induktion, dass für alle $n \in \mathbb{N} \setminus \{0\}$ jeweils n Personen die gleiche Haarfarbe haben. Für $n = 1$ ist dabei die Aussage klar.

Sei nun die Behauptung richtig für ein beliebiges $n \in \mathbb{N} \setminus \{0\}$. Dann ordnen wir $n+1$ Personen in einer Reihe an. Nach Annahme haben die ersten und die letzten n Personen die gleiche Haarfarbe. Mit einer Person P unter diesen ersten und letzten n Personen, gilt die Behauptung für $n + 1$.

Jedoch funktioniert der Induktionsschritt für $n = 1$ nicht, da sich bei 2 Personen keine Person P unter der ersten und letzten $n = 1$ Personen findet.

1.15 Bemerkung

Induktionsbeweise und Widerspruchsbeweise haben oft eine formale Ähnlichkeit. Es wird empfohlen, Widerspruchsbeweise zu vermeiden.

Beispiel (Euklid)

Es gibt unendlich viele Primzahlen.

Beweis durch Widerspruch

Wir nehmen an, es gebe endlich viele Primzahlen $p_1, \ldots, p_n$ und setzen $A = 1 + \prod_{i=1}^{n} p_i$. Sei dann p ein Primteiler von A. Da aber $p_1, \ldots, p_n$ alle Primzahlen sind, gibt es ein $i \in \{1, \ldots, n\}$ mit $p = p_i$. Somit ist $p \neq 1$ ein Teiler von $\prod_{i=1}^{n} p_i$ und daher ein Teiler von 1 – ein Widerspruch.

Beweis durch Induktion

Wir zeigen, dass für alle $n \in \mathbb{N} \setminus \{0\}$ mindestens n verschiedene Primzahlen $p_1, \ldots, p_n$ existieren. Für $n = 1$ wählen wir etwa $p_1 = 2$. Seien nun $p_1, \ldots, p_n$ verschiedene Primzahlen. Da dann $A = 1 + \prod_{i=1}^{n} p_i$ bei Division durch p_i für $1 \leq i \leq n$ den Rest 1 lässt, ist jeder Primteiler p von A verschieden von $p_1, \ldots, p_n$. Wir setzen $p = p_{n+1}$ und erhalten $n+1$ verschieden Primzahlen $p_1, \ldots, p_{n+1}$.

2 Gruppen

2.1 Definition

Eine Gruppe besteht aus einer Menge G und einer Abbildung $(a, b) \in G \times G \longmapsto a \circ b$ mit folgenden Eigenschaften:

1. [Assoziativität] Für alle $a, b, c \in G$ gilt $a \circ (b \circ c) = (a \circ b) \circ c$.
2. [neutrales Element] Es existiert ein $e \in G$ mit $e \circ a = a$ für alle $a \in G$.
3. [Invertierbarkeit] Sei e ein neutrales Element. Für alle $a \in G$ gibt es ein $a' \in G$ mit $a' \circ a = e$.

Dabei schreibt man statt $a \circ b$ auch $a \cdot b$ oder ab. G heißt abelsch oder kommutativ, wenn für alle $a, b \in G$ stets $a \circ b = b \circ a$ gilt. In diesem Fall schreibt man oft $a + b$ statt $a \circ b$.

Bemerkung

1. Da $\circ : G \times G \longrightarrow G$ eine Abbildung ist, ist die Verknüpfung $\circ$ auf G abgeschlossen.
2. Für abelsche Gruppen G nennt man die Verknüpfung $+ : G \times G \longrightarrow G$ eine Summe.

Beispiel

1. $G = \mathbb{Z}$ ist bzgl. $(a, b) \longmapsto a \circ b = a + b$ eine Gruppe, da
   (a) $a + (b + c) = (a + b) + c$
   (b) $0 + a = a$
   (c) $-a + a = 0$
   (d) $a, b \in \mathbb{Z} \Longrightarrow a + b \in \mathbb{Z}$

2. $G = \mathbb{Z}$ ist bzgl. $(a, b) \longmapsto a \circ b = a \cdot b$ keine Gruppe, da

   (a) $1 \cdot a = a$

   (b) $\forall_{a,a' \in G} \quad a \neq 1 \Longrightarrow a' \cdot a \neq 1$

2.2 Satz

Sei G eine Gruppe. Dann gilt:

1. Für jedes neutrale Element $e \in G$ und für alle $a \in G$ gilt $e \circ a = a \circ e = a$.

2. Es gibt genau ein neutrales Element.

3. Aus $ab = e$ folgt $ba = e$.

4. Für alle $a, b \in G$ sind die Gleichungen $ax = b$ und $ya = b$ eindeutig.

Beweis

[3.] Sei e ein neutrales Element und $a' \in G$ mit $a'a = e$. Dann gilt mit $ab = e$ auch $ba = e(ba) = (a'a)(ba) = a'(ab)a = a'ea = a'(ea) = a'a = e$.

[1.] Sei $a' \in G$ mit $a'a = e$. Aus 3 folgt $aa' = e$ und damit $ae = a(a'a) = (aa')a = ea = a$.

[2.] Sei e' ein weiteres neutrales Element. Dann gilt $e' = ee' = e'e = e$.

[4.] Wir betrachten $ax = b$. Sei $a' \in G$ mit $a'a = aa' = e$. Dann ist $x = a'b$ wegen $ax = a(a'b) = (aa')b = eb = b$ eine Lösung. Ist dann x' eine weitere Lösung, so folgt $x = a'b = a'(ax') = (a'a)x' = ex' = x'$.

Nun betrachten wir $ya = b$. Wegen $b = be = b(a'a) = (ba')a$ ist $y = ba'$ eine Lösung. Für $y' \in G$ mit $y'a = b$ folgt dann $y = ba' = (y'a)a' = y'(aa') = y'e = y'$.

Bemerkung

1. Da mit Satz 2.2 die Gleichung $ax = e$ genau eine Lösung hat, ist das Inverse von a eindeutigt bestimmt. Hierfür schreibt man a^{-1}.

2. Wenn G nicht abelsch ist, können die Lösungen für $ax = b$ und $ya = b$ verschieden sein. Daher sollte man $x = a^{-1}b$ und $y = ba^{-1}$ nicht in der Form $\frac{b}{a}$ schreiben.

3. Ist G abelsch und additiv geschrieben, so bezeichnet $-a$ das Inverse von a und man schreibt statt $a + (-b)$ auch $a - b$.

2.3 Korollar

Für alle $a, b \in G$ gilt:

1. $(a^{-1})^{-1} = a$
2. $(ab)^{-1} = b^{-1}a^{-1}$

Beweis

[1.] Wegen $e = a^{-1}a = aa^{-1}$ ist a das Inverse zu a^{-1}.

[2.] Wegen $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = e$ ist $b^{-1}a^{-1}$ das Inverse von ab.

Bemerkung

1. Nur in abelschen Gruppen gilt $(ab)^{-1} = a^{-1}b^{-1}$ bzw. $(ab)^n = a^n b^n$.
2. Eine Gruppe G besteht niemals aus der leeren Menge, da zumindest ein neutrales Element $e \in G$ existiert.
3. Ist G multiplikativ geschrieben, so gilt für $n \in \mathbb{N} \setminus \{0\}$:
   (a) $a^0 = e$
   (b) $a^n = a \cdot \ldots \cdot a$
   (c) $a^{-n} = a^{-1} \cdot \ldots \cdot a^{-1}$
4. Ist G additiv geschrieben, so schreibt man mit $n \in \mathbb{N} \setminus \{0\}$:
   (a) $0 \cdot a = e$
   (b) $n \cdot a = a + \ldots + a$
   (c) $-n \cdot a = a^{-1} + \ldots + a^{-1}$

   Dabei gilt $n \cdot a \neq n \circ a = n + a$.

2.4 Definition

Eine Untergruppe U einer Gruppe G ist eine nichtleere Teilmenge $U \subseteq G$ mit $a, b \in U \Longrightarrow a^{-1} \in U$ und $ab \in U$.

Bemerkung

1. Eine Untergruppe U ist selbst eine Gruppe.

2. Eine Teilmenge $U \subseteq G$ ist dann eine Untergruppe, wenn U nichtleer ist und für alle $a, b \in U$ stets $a, b \in U \Longrightarrow a^{-1}b \in U$ gilt.

Beweis

[1.] Da sich die Verknüpfung $U \times U \longrightarrow U$ von G vererbt, ist die Assoziativität gegeben. Wegen $a, b \in U \Longrightarrow a^{-1} \in U$ und $ab \in U$ ist U gegen Inversen- und Produktbildung abgeschlossen. Mit $a^{-1}, a \in U$ folgt schließlich $e = a^{-1}a \in U$.

[2.] Mit der Verknüpfung verebt sich die Assoziativität. Da U nichtleer ist, existiert ein $a \in U \Longrightarrow e = a^{-1}a \in U$. Mit $a, e \in U$ folgt $a^{-1}e = a^{-1} \in U$ und damit $a, b \in U \Longrightarrow (a^{-1})^{-1}b = ab \in U$.

Beispiel

1. $U = 2\mathbb{Z}$ ist eine Untergruppe von $G = \mathbb{Z}$, da

   (a) $2\mathbb{Z} \neq \emptyset$

   (b) $2k, 2z \in 2\mathbb{Z} \Longrightarrow -2k + 2z = 2(z - k) \in 2\mathbb{Z}$

2. $U = \mathbb{N}$ ist keine Untergruppe von $G = \mathbb{Z}$, da $0 \neq n \in \mathbb{N} \Longrightarrow -n \notin \mathbb{N}$

2.5 Definition

Sei U eine Untergruppe einer Gruppe G. Die Mengen der Form $Ug = \{u \circ g \mid u \in U\}$ heißen Rechtsnebenklassen von U in G. Analog heißt gU Linksnebenklasse.

Bemerkung

1. Für $u \in U$ ist $Uu = U$.

2. Für $g, h \in G$ gilt $U(gh) = (Ug)h$.

Beweis

[1.] Es gilt einerseits $w \in Uu \Longrightarrow w = vu$ mit $v \in U \Longrightarrow w \in U$ – also $Uu \subseteq U$ – und andererseits $w \in U \Longrightarrow wu^{-1} \in U \Longrightarrow w = wu^{-1}u \in Uu$ – also $U \subseteq Uu$.

[2.] Es gilt $w \in U(gh) \Longleftrightarrow w = u(gh) = (ug)h$ für ein $u \in U \Longleftrightarrow w \in (Ug)h$.

2.6 Lemma

1. Durch $g \sim h \Longleftrightarrow Ug = Uh$ wird eine Äquivalenzrelation auf G definiert.
2. Die Äquivalenzklasse von $g \in G$ ist genau die Rechtsnebenklasse Ug.

Beweis

[1.] Reflexivität, Symmetrie und Transitivität folgen unmittelbar aus der Gleichheit $Ug = Uh$.

[2.] Sei $[g]$ die Äquivalenzklasse von g. Dann folgt $h \in [g] \Longrightarrow Uh = Ug$. Wegen $e \in U$ gilt $h \in Uh$, also $h \in Ug$.

Andererseits gilt $h \in Ug \Longrightarrow h = ug$ für ein $u \in U$. Es folgt $Uh = U(ug) = (Uu)g = Ug$, also $h \in [g]$.

2.7 Lemma

Für alle $g \in G$ gilt $|Ug| = |U|$.

Beweis

Wir betrachten die Abbildung $\varphi : u \in U \longmapsto ug \in Ug$.

Sei $u, w \in U$ – dann folgt $ug = \varphi(u) = \varphi(w) = wg \Longrightarrow u = ugg^{-1} = wgg^{-1} = w$, d.h. φ ist injektiv. Weiter gilt $v \in Ug \Longrightarrow v = ug$ für $u \in U \Longrightarrow v = \varphi(u)$, d.h. φ ist surjektiv.

Da also φ bijektiv ist, gilt $|Ug| = |U|$.

2.8 Satz von Lagrange

Sei U eine Untergruppe der endlichen Gruppe G. Dann ist $|U|$ ein Teiler von $|G|$.

Beweis

Die Äquivalenzklassen aus Lemma 2.6. bilden nach Lemma 1.7 eine disjunkte Zerlegung von G. Da G nur endlich viele Elemente hat, folgt $|G| = |Ug_1| + \ldots + |Ug_n| = n \cdot |U|$ für ein $n \in \mathbb{N}$. Somit ist $|U|$ ein Teiler von $|G|$.

2.9 Definition

Eine Untergruppe $N \leq G$ heißt Normalteiler, wenn für alle $g \in G$ stets $gN = Ng$ gilt.

2.10 Bemerkung

Eine Untergruppe $N \leq G$ ist genau dann ein Normalteiler, wenn für alle $g \in G$ stets $g^{-1}Ng \subseteq N$ gilt.

Beweis

[1.] Es gelte $g^{-1}Ng \subseteq N$ für alle $g \in G$ und es sei $ng \in Ng$ mit $n \in N$. Dann ist $g^{-1}ng \in g^{-1}Ng \subseteq N$, d.h. $g^{-1}ng = m$ für ein $m \in N \Longrightarrow ng = gm \in gN$.

Sei nun $gm \in gN$ für $m \in N$. Wegen $g = h^{-1}$ mit $h = g^{-1}$ folgt $gmg^{-1} \in h^{-1}Nh \subseteq N \Longrightarrow gmg^{-1} = n$ für ein $n \in N$. Also ist $gm = ng \in Ng$.

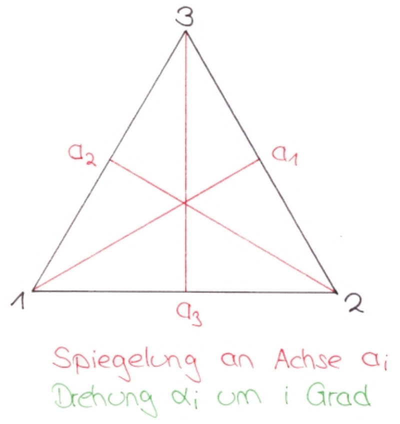
Insgesamt sieht man $gN = Ng$ für ein beliebiges Element $g \in G$.

[2.] Sei N normal in G und $g^{-1}ng \in g^{-1}Ng$ mit $n \in N$. Dann ist $ng \in Ng = gN$, d.h. $ng = gm$ für ein $m \in N$. Es folgt $g^{-1}ng = g^{-1}gm = m \in N$.

Beispiel

1. In abelschen Gruppen ist jede Untergruppe ein Normalteiler.

2. Sei G die Menge der Symmetrien eines gleichseitigen Dreiecks,



d.h. $G = \{a_1, a_2, a_3, \alpha_{120}, \alpha_{240}, \alpha_{360}\}$. Dann ist G bzgl. der Hintereinanderausführung der Abbildungen eine Gruppe mit neutralem Element α_{180}.

(a) Sei nun N die Menge aller gleichsinnigen Symmetrien, also $N = \{\alpha_{120}, \alpha_{240}, \alpha_{360}\}$. Dann ist N ein Normalteiler, obwohl G nicht abelsch ist:

Sei zunächst $g \in N$. Dann ist auch $g^{-1} \in N$ und es gilt $g^{-1}Ng = g^{-1}N = N$. Sei nun $g \notin N$. Dann sind g und g^{-1} Achsenspiegelungen, d.h. $g^{-1}ng$ ist für eine beliebige Drehung $n \in N$ wieder eine Drehung, d.h. $g^{-1}ng \in N$.

(b) Sei $U = \{a_1, \alpha_{360}\}$ eine Untergruppe von G. Dann ist U kein Normalteiler von G:

Es gilt $a_2^{-1}a_1a_2(1) = 2$, $a_2^{-1}a_1a_2(2) = 1$ und $a_2^{-1}a_1a_2(3) = 3$ – also $a_2^{-1}a_1a_2 = a_3$. Damit folgt $a_2^{-1}Ua_2 \nsubseteq U$.

2.11 Definition / Satz

Sei N ein Normalteiler von G. Auf der Menge der Nebenklassen $G|_N$ von N in G wird durch $(Nx)(Ny) = Nxy$ ein Produkt definiert, dass $G|_N$ zu einer Gruppe mit neutralem Element N macht. Dabei heißt $G|_N$ Faktor- oder Quotientengruppe.

Beweis

Es ist zunächst zu zeigen, dass das Produkt wohldefiniert ist – d.h. $N\widetilde{x} = Nx$ und $N\widetilde{y} = Ny \Longrightarrow (N\widetilde{x})(N\widetilde{y}) = (Nx)(Ny) = Nxy$. Wegen $\widetilde{x} \in N\widetilde{x} = Nx$ ist $\widetilde{x} = nx$ mit $n \in N$. Analog ist $\widetilde{y} = my$ für ein $m \in N$. Da N normal ist, folgt $(N\widetilde{x})(N\widetilde{y}) = N\widetilde{x}\widetilde{y} = Nnxmy = Nxmy = xNmy = xNy = Nxy$.

Es gilt mit $n \in N$ weiter $N(Nx) = (Nn)(Nx) = Nnx = Nx$, d.h. N ist ein neutrales Element. Wegen $(Nx^{-1})(Nx) = Nx^{-1}x = Ne = N$ ist $G\,|_N$ abgeschlossen gegen Inversenbildung. Die Assoziativität überträgt sich von G.

Beispiel

Sei $G = (\mathbb{Z}, +)$ die Gruppe der ganzen Zahlen und sei $n \in \mathbb{N}$. Dann ist $U = n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ ein Normalteiler der abelschen Gruppe G. Wir betrachten nun die Faktorgruppe $\mathbb{Z}\mid_{n\mathbb{Z}}$.

Nach Lemma 2.6 und Lemma 1.7 sind zwei Nebenklassen $n\mathbb{Z} + g = Ug$ und $n\mathbb{Z} + h = Uh$ disjunkt oder identisch. Wegen $n\mathbb{Z} + g = n\mathbb{Z} + h \iff g \in n\mathbb{Z} + h \iff g = nz + h$ für ein $z \in \mathbb{Z} \iff g - h = nz \iff n$ teilt $g - h$ besteht dann $\mathbb{Z}\mid_{n\mathbb{Z}}$ aus den Elementen $n\mathbb{Z}, n\mathbb{Z} + 1, \ldots, n\mathbb{Z} + (n - 1)$.

2.12 Definition

Seien G, H Gruppen. Eine Abbildung $\varphi : G \longmapsto H$ heißt (Gruppen-)Homomorphismus, falls $\varphi(a \circ b) = \varphi(a) \circ \varphi(b)$ für alle $a, b \in G$ gilt.

φ heißt Monomorphismus bzw. Epimorphismus bzw. Isomorphismus, falls φ injektiv bzw. surjektiv bzw. bijektiv ist. G und H heißen isomorph, falls es einen Isomorphismus $G \longrightarrow H$ gibt. Ein Endomorphismus ist ein Homomorphismus $G \longrightarrow G$.

Bemerkung

1. Sei e_G bzw. e_H das neutrale Element der Gruppe G bzw. H und sei $\varphi : G \longmapsto H$ homomorph. Dann gilt $\varphi(e_G) = \varphi(e_G \circ e_G) = \varphi(e_G) \circ \varphi(e_G) \iff e_H = \varphi(e_G)^{-1} \circ \varphi(e_G) = \varphi(e_G)^{-1} \circ \varphi(e_G) \circ \varphi(e_G) = \varphi(e_G)$.

2. Sei weiter $g \in G$ beliebig. Wegen $e_H = \varphi(e_G) = \varphi(g - 1 \circ g) = \varphi(g - 1) \circ \varphi(g)$ ist $\varphi(g - 1) = \varphi(g)^{-1}$. Allgemein folgt $\varphi(g^n) = \varphi(g)^n$ für alle $n \in \mathbb{Z}$.

Beispiel

1. $x \longmapsto \mathrm{e}^x$ ist wegen $\mathrm{e}^{x+y} = \mathrm{e}^x \cdot \mathrm{e}^y$ ein Monomorphismus der Gruppen $(\mathbb{R}, +)$ und $(\mathbb{R}\backslash\{0\}, \cdot)$.

2. Sei N ein Normalteiler der Gruppe G. Dann ist $g \in G \longmapsto Ng \in G|_N$ wegen $Ngh = NgNh$ ein Epimorphismus. Diese Abbildung wird als natürlicher Homomorphismus bezeichnet.

3. Alle Gruppen mit zwei Elementen sind isomorph:

   Gruppen mit genau zwei Elementen bestehen aus einem neutralen und einem selbstinversen Element. Wir betrachten $G = \{e_G, a\}$ und $H = \{e_H, b\}$ sowie $\varphi : G \longrightarrow H$ definiert durch $\varphi(e_G) = e_H$ und $\varphi(a) = b$. Dann gilt etwa $\varphi(aa) = \varphi(e_G) = e_H = bb = \varphi(a)\varphi(a)$.

2.13 Definition / Lemma

Der Kern eines Homomorphismus $\varphi : G \longrightarrow H$ besteht aus den Elementen $g \in G$ mit $\varphi(g) = e_H$. Kern φ ist ein Normalteiler von G.

Beweis

Bezeichne $K = \text{Kern } \varphi$. Wegen $\varphi(e_G) = e_H$ ist $K \neq \emptyset$. Sei nun $a, b \in K$, d.h. $\varphi(a) = \varphi(b) = e_H$. Es folgt $\varphi(a \cdot b^{-1}) = \varphi(a) \cdot \varphi(b)^{-1} = e_H \cdot e_H^{-1} = e_H$, also $a \cdot b^{-1} \in K$. Insgesamt ist K eine Untergruppe von G.

Sei $g^{-1}kg \in g^{-1}Kg$ mit $g \in G$ und $k \in K$ beliebig. Wegen $\varphi(g^{-1}kg) = \varphi(g^{-1}) \cdot \varphi(k) \cdot \varphi(g) = \varphi(g^{-1}) \cdot e_H \cdot \varphi(g) = \varphi(g^{-1}) \cdot \varphi(g) = \varphi(g^{-1}g) = \varphi(e_G) = e_H$ ist dann auch $g^{-1}kg \in K$. Daher ist K normal in G.

2.14 Lemma

Sei $\varphi : G \longrightarrow H$ ein Gruppenhomomorphismus. Dann gilt: φ injektiv $\Longleftrightarrow$ Kern $\varphi = \{e_G\}$.

Beweis

Sei zunächst φ injektiv und $g \in \text{Kern } \varphi$. Es folgt $\varphi(g) = e_H = \varphi(e_G) \Longrightarrow g = e_G$.

Sei nun Kern $\varphi = \{e_G\}$ und $g, h \in G$ beliebig mit $\varphi(g) = \varphi(h)$. Dann gilt $e_H = \varphi(g)^{-1}\,\varphi(h) = \varphi(g^{-1}h) \Longrightarrow g^{-1}h \in \text{Kern } \varphi \Longrightarrow g^{-1}\,h = e_G \Longrightarrow g = h$.

Bemerkung

Sei N ein Normalteiler von G und $\varphi : g \in G \longmapsto Ng \in G|_N$ der natürliche Homomorphismus. Dann gilt Kern $\varphi = \{g \in G \mid \varphi(g) = N\} = \{g \in G \mid Ng = N\} = \{g \in G \mid g \in N\} = N$.

2.15 Satz (Homomorphiesatz)

Sei $\varphi : G \longrightarrow H$ ein Epimorphismus und bezeichne $K = \text{Kern } \varphi$. Dann sind die Gruppen $G\,|_K$ und H isomorph. Ein Isomorphismus ist durch $\overline{\varphi} : Kg \in G\,|_K \longmapsto \varphi(g)$ gegeben.

Beweis

Sei zuerst $Kg = Kh$ für $g, h \in G$, d.h. $g = kh$ für ein $k \in K$. Dann gilt $\overline{\varphi}(Kg) = \varphi(g) = \varphi(kh) = \varphi(k)\,\varphi(h) = e_H\,\varphi(h) = \varphi(h) = \overline{\varphi}(Kh)$ – also ist $\overline{\varphi}$ wohldefiniert.

Wegen $\overline{\varphi}(Kg\,Kh) = \overline{\varphi}(Kgh) = \varphi(gh) = \varphi(g)\,\varphi(h) = \overline{\varphi}(Kg)\,\overline{\varphi}(Kh)$ ist $\overline{\varphi}$ ein Homomorphismus.

Nun betrachten wir Kern $\overline{\varphi}$. Mit $Kg \in \text{Kern}\,\overline{\varphi} \Longrightarrow \varphi(g) = e_H \Longrightarrow g \in K \Longrightarrow Kg = K$ folgt Kern $\overline{\varphi} = \{K\}$, d.h. $\overline{\varphi}$ ist injektiv.

Da zuletzt φ ein Epimorphismus ist, ist auch $\overline{\varphi}$ surjektiv.

2.16 Definition / Bemerkung

Sei M eine nichtleere Menge. Dann ist $\text{Sym}(M)$ die Menge aller Bijektionen $M \longrightarrow M$ und bildet bzgl. der Hintereinanderausführung der Abbildungen eine Gruppe. $\text{Sym}(M)$ wird als symmetrische Gruppe bezeichnet.

Ist M endlich, so heißt ein Element $\pi \in \text{Sym}(M)$ eine Permutation. Für $M = \{1, \ldots, n\}$ schreibt man S_n statt $\text{Sym}(M)$.

Beweis

Sei $m \in M$. Die Verknüpfung $\alpha \circ \beta(m) = \alpha\big(\beta(m)\big)$ ist offenbar assoziativ. Das neutrale Element ist die identische Abbildung $m \longmapsto m$ und das Inverse einer Bijektion $\alpha \in \text{Sym}(M)$ ist die Umkehrabbildung $\alpha(m) \longmapsto m$.

Bemerkung

S_1 und S_2 sind kommutativ. Für alle $n \geq 3$ ist S_n nicht abelsch.

Beweis

S_1 besteht nur aus der identischen Abbildung id. S_2 besitzt zwei Elemente: α und id mit $\text{id} \circ \alpha = \alpha \circ \text{id}$.

Für alle $n \geq 3$ gilt $\alpha, \beta \in S_n$ mit

$$\begin{aligned} \alpha(1) &= 2 & \beta(1) &= 1 \\ \alpha(2) &= 1 & \beta(2) &= 3 \\ \alpha(3) &= 3 & \beta(3) &= 2 \end{aligned}$$

und $\alpha(n) = \beta(n) = n$ für $n \geq 4$. Es folgt $\alpha \circ \beta(1) = 2 \neq 3 = \beta \circ \alpha(1)$.

2.17 Definition

Sei $\delta \in S_n$ eine Permutation mit $\delta(a_1) = a_2, \ldots, \delta(a_r) = a_1, \delta(b_1) = b_2, \ldots, \delta(b_s) = b_1, \ldots$ für $a_i, b_i, \ldots \in \{1, \ldots, n\}$. Dann wird δ in Zykelnotation durch $(a_1 \cdots a_r)(b_1 \cdots b_s) \cdots$ dargestellt. Zykel der Länge 1 lässt man weg. Ein Spezialfall der Form $\delta = (a_1 \cdots a_m)$ heißt m-Zykel.

Bemerkung

1. Die Permutation $\delta = (a_1 \cdots a_r)(b_1 \cdots b_s)$ ist ein Produkt $\alpha \circ \beta$ der Zykel $\alpha = (a_1 \cdots a_r)$ und $\beta = (b_1 \cdots b_s)$.

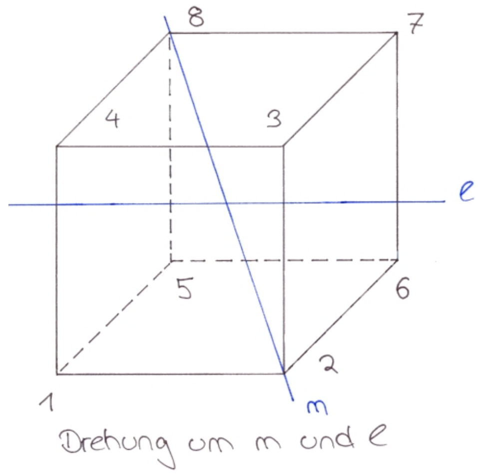
2. Da δ eine Bijektion ist, sind die Mengen $\{a_i\}$ und $\{b_i\}$ der Zykelnotation paarweise disjunkt. Somit gilt $\delta(i) = \alpha \circ \beta(i) = \beta \circ \alpha(i)$ für alle $i \in \{1, \ldots, n\}$, d.h.

$$(a_1 \cdots a_r)(b_1 \cdots b_s) = (b_1 \cdots b_s)(a_1 \cdots a_r).$$

   Allgemein kommutieren disjunkte Zykel bei einem Produkt $\delta \circ \gamma$ mit $\delta, \gamma \in S_n$.

3. Die Positionen eines Zykels sind bis auf Reihenfolge beliebig, d.h. $(abc) = (bca) = (cab)$.

Beispiel



Die Drehung um m wird durch $\delta = (136)(475)$ und die Drehung um l durch $\tau = (2376)(1485)$ dargestellt. Für das Produkt gilt $\delta \circ \tau = (136)(475)\,(2376)(1485) = (17)(26)(35)(48)$.

2.18 Lemma

Für $\delta \in S_n$ gibt es ein $0 < k \in \mathbb{N}$ mit $\delta^k = \mathrm{id}$.

Beweis

Es gilt $|S_n| = n!$. Man betrachte nun die $n! + 1$ Elemente $\delta, \delta^2, \ldots, \delta^{n!+1}$. Da S_n eine Gruppe ist, gilt $\delta^l \in S_n$ für alle $l \in \mathbb{N}$. Daher sind mindestens zwei Permutationen δ^i und δ^j für $0 < i < j \leq n! + 1$ gleich.

Es folgt für das neutrale Element $\mathrm{id} = e = \delta^i \cdot (\delta^i)^{-1} = \delta^j \cdot (\delta^{-1})^i = \delta^{j-i}$. Setze $k = j - i > 0$.

2.19 Definition

Eine Transposition $\tau \in S_n$ ist eine Permutation, die nur zwei Elemente vertauscht – also $\tau = (ab)$ für $a \neq b$.

2.20 Satz

Jede Permutation $\delta \in S_n$ ist Produkt von Transpostionen.

Beweis

Da jede Permutation ein Produkt disjunkter Zykel ist, genügt es $\delta = (a_1 \cdots a_m)$ zu untersuchen. Für $m = 1$ ist $\delta = \mathrm{id}$ mit $\mathrm{id} = (a_1 a_2)(a_2 a_1)$. Sei nun ein $(m-1)$-Zykel Produkt von Transpositionen. Die Behauptung folgt dann durch vollständige Induktion aus $(a_1 \cdots a_m) = (a_1 a_2)(a_2 \cdots a_m)$.

Bemerkung / Definition

1. Die Darstellung einer Permutation als Produkt von Transpositionen ist nicht eindeutig, etwa ist $(ba)(bc)(bc)(bc) = (abc) = (ac)(ab)$.

2. Für $\delta \in S_n$ seien $m_1, \ldots, m_k$ die Zykellängen. Setze $f(\delta) = \sum\limits_{i=1}^{k}(m_i - 1)$.

3. Für $a, b \in \mathbb{Z}$ bedeutet $a \equiv b \pmod 2$, dass $a + b$ durch 2 teilbar ist.

2.21 Lemma

Sei $\delta \in S_n$ ein Produkt von m Transpositionen. Dann ist $m \equiv f(\delta) \pmod 2$.

Beweis

Wir beweisen die Aussage durch vollständige Induktion über m. Für $m = 1$ ist dabei δ eine Transposition mit $f(\delta) = 1$ – also ist die Behauptung klar.

Sei nun $\delta = \tau_1 \cdot \ldots \cdot \tau_{m+1}$ Produkt von $m+1$ Transpositionen. Wir setzen $\alpha = \tau_1 \cdot \ldots \cdot \tau_m$, d.h. $\delta = \alpha \cdot \tau_{m+1}$ und nehmen an, es gilt $m \equiv f(\alpha) \pmod 2$. Sei zudem $\tau_{m+1} = (uv)$ mit $u \neq v$. Dann unterscheiden wir zwei Fälle.

1 Es kommen u und v im gleichen Zykel von α vor. Dieser Zykel sei $(a_1 \cdots a_r)$ mit $a_r = u$ sowie $a_j = v$ für $1 \leq j < r$ und trete in der Notation von α zuletzt auf.

Wir berechnen $(a_1 \cdots a_r) \cdot \tau_{m+1} = (a_1 \cdots a_r)(a_r a_j) = (a_1 \cdots a_j)(a_{j+1} \cdots a_r)$. Da sich dann α und $\alpha \cdot \tau_{m+1}$ nur in den letzten Zyklen $(a_1 \cdots a_r)$ bzw. $(a_1 \cdots a_j)(a_{j+1} \cdots a_r)$ unterscheiden, folgt

$$f(\alpha \cdot \tau_{m+1}) - f(\alpha) = \big[(j-1) + \big((r-j)-1\big)\big] - (r-1) = -1.$$

Damit ergibt sich $f(\delta) + (m+1) = f(\alpha \cdot \tau_{m+1}) + (m+1) = f(\alpha) - 1 + (m+1) = f(\alpha) + m$ und mit der Induktionsannahme folgt $f(\delta) \equiv m+1 \pmod 2$.

2 Nun liegen u und v in verschiedenen Zykeln von α. Diese Zykel mögen in der Notation zuletzt auftreten und seien durch $(a_1 \cdots a_r)$ mit $a_r = u$ und $(b_1 \cdots b_s)$ mit $b_s = v$ gegeben. Dies beinhaltet dabei auch den Fall, dass u oder v in „keinem“ Zykel – d.h. in Zykeln der Länge 1 – vorkommen.

Analog zu 1 vergleichen wir $(a_1 \cdots a_r)(b_1 \cdots b_s)$ mit $(a_1 \cdots a_r)(b_1 \cdots b_s) \cdot \tau_{m+1} = (a_1 \cdots a_r)(b_1 \cdots b_s)(a_r b_s) = (a_1 \cdots a_r b_1 \cdots b_s)$. Es folgt

$$f(\alpha \cdot \tau_{m+1}) - f(\alpha) = \big[(r+s)-1\big] - \big[(r-1)+(s-1)\big] = 1,$$

d.h. $f(\delta) + (m+1) = f(\alpha) + m + 2$. Nach Annahme ist $f(\alpha) + m$ durch 2 teilbar, also auch $f(\alpha) + m + 2 \Longrightarrow f(\delta) \equiv m+1 \pmod 2$.

2.22 Satz

Die Signum-Funktion $\mathrm{sign} : \delta \in S_n \longmapsto (-1)^{f(\delta)} \in \{1, -1\}$ ist ein Gruppenhomomorphismus.

Beweis

Die Menge $\{1, -1\}$ ist bzgl. der Multiplikation eine Gruppe mit neutralem Element 1.

Seien nun α bzw. β Produkt von r bzw. s Transpositionen, d.h. $\alpha \circ \beta$ ist Produkt von $r + s$ Transpositionen. Mit Lemma 2.21 sind $f(\alpha)$ und r entweder beide gerade oder ungerade, also $(-1)^{f(\alpha)} = (-1)^r$. Analog ist $(-1)^{f(\beta)} = (-1)^s$ und $(-1)^{f(\alpha\circ\beta)} = (-1)^{r+s}$.

Damit folgt $\mathrm{sign}(\alpha \circ \beta) = (-1)^{r+s} = (-1)^r \cdot (-1)^s = \mathrm{sign}(\alpha) \cdot \mathrm{sign}(\beta)$.

2.23 Definition / Bemerkung

Der Kern von sign bildet als Normalteiler von S_n die alternierende Gruppe A_n. Eine Permutation $\delta \in$ Kern sign, d.h. $\mathrm{sign}(\delta) = 1$, heißt gerade und eine Permutation $\delta \notin$ Kern sign heißt ungerade. Nach Lemma 2.21 ist eine gerade Permutation durch eine gerade Anzahl von Transpositionen darstellbar.

Beispiel

Mit $\mathrm{id} = 1$ ist $S_3 = \{1, (12), (13), (23), (123), (321)\}$ und $A_3 = \{1, (123), (321)\}$.

3 Ringe und Körper

3.1 Definition

Sei $(R, +)$ eine abelsche Gruppe und sei ein Produkt $\cdot : R \times R \longrightarrow R$ definiert. Dann heißt R ein Ring, wenn gilt:

1. Das Produkt ist assoziativ und besitzt ein neutrales Element.
2. Es gelten die Distributivgesetze $a \cdot (b + c) = a \cdot b + a \cdot c$ und $(a + b) \cdot c = a \cdot c + b \cdot c$.

R heißt kommutativ, wenn für alle $a, b \in R$ stets $a \cdot b = b \cdot a$ gilt.

Bemerkung

Für einen Ring R bezeichnet man die Summe bzw. das Produkt als Addition bzw. Multiplikation. Das jeweilige neutrale Element wird mit 0 bzw. 1 bezeichnet.

3.2 Definition

Ein Ring R heißt nullteilerfrei, wenn für alle $a, b \in R$ aus $ab = 0$ stets $a = 0$ oder $b = 0$ folgt.

Beispiel

$R = \mathbb{Z}$ bildet mit Addition und Multiplikation einen nullteilerfreien, kommutativen Ring.

3.3 Lemma

In einem Ring R gilt für alle $a, b, c \in R$:

1. $0a = a0 = 0$
2. $(-a)b = a(-b) = -(ab)$
3. $a(b - c) = ab - ac$ und $(a - b)c = ac - bc$.
4. $0 = 1 \Longrightarrow R = \{0\}$

Beweis

1 Es gilt $0a = (0 + 0)a = 0a + 0a$, also ist $0a$ das neutrale Element der Addition. Analog folgt $a0 = 0$.

2 Wegen $(-a)b + ab = (-a + a)b = 0b = 0$ ist $(-a)b = -(ab)$. Ebenso gilt $a(-b) = -(ab)$.

3 Es gilt $a(b - c) = a(b + (-c)) = ab + a(-c) = ab + (-(ac)) = ab - ac$ und analog $(a - b)c = ac - bc$.

4 Sei $0 = 1$ und $a \in R$. Dann gilt $a = 1 \cdot a = 0 \cdot a = 0$.

3.4 Definition

Seien S und R Ringe. Ein Ringhomomorphismus ist eine Abbildung $\varphi : R \longrightarrow S$, so dass

1. $\varphi(1) = 1$
2. $\varphi(a + b) = \varphi(a) + \varphi(b)$
3. $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

für alle $a, b \in R$ gilt.

Bemerkung

φ ist offenbar ein Gruppenhomomorphismus der abelschen Gruppen $(S,+)$ und $(R,+)$. Daher gilt $\varphi(0) = 0$.

3.5 Definition

Ein Ideal eines kommutativen Ringes R ist eine Teilmenge $I \subseteq R$, so dass $(I,+)$ eine Untergruppe von $(R,+)$ ist und $r \cdot i \in I$ für alle $r \in R$ und $I \in I$ gilt.

Bemerkung

Sei $\varphi : R \longrightarrow S$ ein Homomorphismus kommutativer Ringe und sei $I = \text{Kern } \varphi = \{r \in R \mid \varphi(r) = 0\}$. Dann ist $(I,+)$ nach Lemma 2.13 eine Untergruppe von $(R,+)$. Wegen $\varphi(r \cdot i) = \varphi(r) \cdot \varphi(i) = \varphi(r) \cdot 0 = 0$ – also $r \cdot i \in I$ – für alle $r \in R$ und $i \in I$, ist I ein Ideal von R.

Beispiel

Sei I ein Ideal von $R = \mathbb{R}$. Sei $0 \neq i \in I$, d.h. insbesondere $\frac{1}{i} \in R$. Es folgt $1 = \frac{1}{i} \cdot i \in I$ und daher $r \cdot 1 \in I$ für alle $r \in R$. Daher gilt entweder $I = \{0\}$ oder $I = R$.

3.6 Definition / Satz

Sei I ein Ideal eines kommutativen Ringes R und $R\mid_I$ die Faktorgruppe der abelschen Gruppen $(R,+)$ und $(I,+)$ mit der Summe $(I+x)+(I+y) = I+(x+y)$.

Dann wird durch $(I+x)\cdot(I+y) = I+(x\cdot y)$ auf $R\mid_I$ ein Produkt definiert, dass $R\mid_I$ zu einem Ring macht. Die Abbildung $\varphi : r \in R \longmapsto I + r \in R\mid_I$ ist dabei ein Ringhomomorphismus.

Beweis

Zunächst zeigen wir, dass das Produkt wohldefiniert ist. Seien dazu $x, \widetilde{x}, y, \widetilde{y} \in R$ mit $I + x = I + \widetilde{x}$ und $I + y = I + \widetilde{y}$ gegeben, d.h. $\widetilde{x} = x + i$ und $\widetilde{y} = y + j$ für $i, j \in I$. Dann gilt $\widetilde{x} \cdot \widetilde{y} = (x+i)\cdot(y+j) = xy + iy + xj + ij$ mit iy, xj und $ij \in I$, also $\widetilde{x} \cdot \widetilde{y} = k + xy$ für ein $k \in I$. Es folgt $(I+\widetilde{x})\cdot(I+\widetilde{y}) = I+(\widetilde{x}\cdot\widetilde{y}) = I+(k+x\cdot y) = I+(x\cdot y) = (I+x)\cdot(I+y)$.

Die Assoziativität des Produkts ergibt sich durch $\big((I+x)(I+y)\big)(I+z) = J+(xy)z = J+x(yz) = (I+x)\big((I+y)(I+z)\big)$ aus der Assozitivität in R. Analog folgt die Existenz des neutralen Elements der Multiplikation und die Distributivität.

Zuletzt folgt aus der Definition der Summe und des Produkts $\varphi(1) = J + 1$ sowie $\varphi(x + y) = \varphi(x) + \varphi(y)$ und $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$.

Beispiel

Sei $R = \mathbb{Z}$ der Ring der ganzen Zahlen. Dann ist $I = n\mathbb{Z}$ für $n \in \mathbb{N}$ eine additive Untergruppe von R. Sei nun $r \in R$ und $nz \in I$, d.h. $z \in R$. Es folgt $r(nz) = n(rz) \in I$, also ist I ein Ideal. Nach Satz 3.6 bildet also $R\,|_I = \mathbb{Z}\,|_{n\mathbb{Z}}$ den sog. Restklassenring.

Wir betrachten nun $\mathbb{Z}\,|_{4\mathbb{Z}} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ mit $\overline{i} = 4\mathbb{Z} + i$ für $0 \leq i \leq 3$. Mit $4\mathbb{Z} + i = 4\mathbb{Z} + j \iff$ 4 teilt $i - j$ ergibt sich folgende Multiplikationstabelle:

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

3.7 Definition

Ein kommutativer Ring K mit $0 \neq 1$ heißt Körper, wenn es für alle $a \in K \setminus \{0\}$ ein $b \in K$ mit $ab = 1$ gibt.

3.8 Bemerkung

1. Körper sind nullteilerfrei.

2. Ein Ring R ist genau dann ein Körper, wenn $(R \setminus \{0\}, \cdot)$ eine abelsche Gruppe bildet.

Beweis

1 Sei K ein Körper und seien $a, b \in K$ mit $a \neq 0$ sowie $ab = 0$. Dann ist a invertierbar und es folgt $0 = a^{-1}0 = a^{-1}ab = b$.

2 Sei $(R \setminus \{0\}, \cdot)$ eine abelsche Gruppe. Dann ist R kommutativ und $(R \setminus \{0\}, \cdot)$ gegen Inversenbildung abgeschlossen.

Sei nun R ein Körper. Da dann R nullteilerfrei ist, ist die Einschränkung des Produkts auf $R \setminus \{0\}$ wohldefiniert. Insbesondere ist R ein kommutativer Ring, d.h. für die Multiplikation folgt Assoziativität und Existenz eines neutralen Elements. Mit der Definition ist R gegen Inversenbildung abgeschlossen.

Beispiel

$\mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ sind Körper.

3.9 Satz

Sei p eine Primzahl. Dann ist $\mathbb{F}_p = \mathbb{Z} \mid_{p\mathbb{Z}}$ ein Körper mit genau p Elementen.

Beweis

Wegen Satz 3.6 ist $\mathbb{F}_p$ ein Ring mit p Elementen.

Ein Element aus $\mathbb{F}_p$ ist eine Nebenklasse $p\mathbb{Z}+i$ für $0 \leq i \leq p-1$. Schreibe $p\mathbb{Z}+i = \overline{i}$. Dann gilt $\overline{a}+\overline{b} = (p\mathbb{Z}+a)+(p\mathbb{Z}+b) = p\mathbb{Z}+(a+b) = \overline{a+b}$ und $\overline{a}\cdot\overline{b} = (p\mathbb{Z}+a)\cdot(p\mathbb{Z}+b) = p\mathbb{Z}+(a\cdot b) = \overline{a \cdot b}$. Weiter gilt $\overline{i} = \overline{0} \Longleftrightarrow p\mathbb{Z} + i = p\mathbb{Z} \Longleftrightarrow i \in p\mathbb{Z} \Longleftrightarrow i = pz$ für ein $z \in \mathbb{Z} \Longleftrightarrow p$ teilt i.

Wir zeigen nun, dass für alle $\overline{0} \neq \overline{a} \in \mathbb{F}_p$ ein $\overline{b} \in \mathbb{F}_p$ existiert mit $\overline{a}\overline{b} = 1$. Dazu betrachten wir die Abbildung $\varphi : \overline{x} \in \mathbb{F}_p \longmapsto \overline{a} \cdot \overline{x}$ mit $\overline{a} \neq \overline{0}$. Dann ist p kein Teiler von a.

Sei $\varphi(\overline{x}) = \varphi(\overline{y})$. Dann folgt $\overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{y}$, d.h. $\overline{a \cdot (x-y)} = \overline{a \cdot x - a \cdot y} = \overline{a \cdot x} - \overline{a \cdot y} = \overline{a} \cdot \overline{x} - \overline{a} \cdot \overline{y} = \overline{0}$. Daher ist p ein Teiler von $a \cdot (x-y)$ und da p ein Primzahl und kein Teiler von a ist, ist p ein Teiler von $x - y$. Somit gilt $\overline{x} - \overline{y} = \overline{x-y} = \overline{0}$, d.h. $\overline{x} = \overline{y}$. Insgesamt ist φ also injektiv.

Da aber φ eine injektive Abbildung $\mathbb{F}_p \longrightarrow \mathbb{F}_p$ ziwschen endlichen Mengen ist, ist φ sogar surjektiv. Damit existiert ein $\overline{b} \in \mathbb{F}_p$ mit $\overline{a} \cdot \overline{b} = \varphi(b) = \overline{1}$.

4 Vektorräume

4.1 Definition

Sei K ein Körper und $(V, +)$ eine abelsche Gruppe. Dann heißt V Vektorraum über K bzw. K-Vektorraum, wenn es eine Abbildung $(\lambda, v) \in K \times V \longrightarrow \lambda \cdot v \in V$ gibt, mit

1. [gemischte Assoziativität] für alle $\lambda, \mu \in K$ und $v \in V$ gilt $(\lambda \cdot \mu) \cdot v = \lambda \cdot (\mu \cdot v)$

2. [gemischte Distributivität] für alle $\lambda, \mu \in K$ und $v, w \in V$ gilt $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$ und $\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$

3. [Normierung] für $1 \in K$ und alle $v \in V$ gilt $1 \cdot v = v$

Dabei heißt ein Element $\lambda \in K$ bzw. $v \in V$ ein Skalar bzw. Vektor. Das Element $0 \in V$ wird als Nullvektor bezeichnet und $V = \{0\}$ heißt Nullraum.

Bemerkung

Sei V ein K-Vektorraum. Allgemein sind dann die Verknüpfungen $+ : K \times K \longrightarrow K$ und $+ : V \times V \longrightarrow V$ bzw. $\cdot : K \times K \longrightarrow K$ und $\cdot : K \times V \longrightarrow V$ verschieden. Daher bezeichnet man etwa $(\lambda \cdot \mu) \cdot v = \lambda \cdot (\mu \cdot v)$ als „gemischte" Assoziativität.

Bemerkung

Sei K ein Körper und $0 < n \in \mathbb{N}$. Auf V seien dann die Verknüpfungen $(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$ und $a \cdot (a_1, \ldots, a_n) = (a \cdot a_1, \ldots, a \cdot a_n)$ definiert. Dann bildet V einen K-Vektorraum.

Beweis

Da K ein Körper und die Summe komponentenweise definiert ist, ist $(V, +)$ eine abelsche Gruppe. Die Vektorraumaxiome folgen ebenso aus der Körperstruktur von K.

Beispiel

1. K^n mit $0 < n \in \mathbb{N}$ und $K = \mathbb{F}_p$ für eine Primzahl p ist ein Vektorraum mit genau p^n Elementen.

2. Sei $M \neq \emptyset$ eine Menge und K ein Körper. Dann ist $V = \{f : M \longrightarrow K \mid f \text{ ist Abbildung}\}$ bzgl. $(f + g)(m) = f(m) + g(m)$ eine abelsche Gruppe. Durch $(a \cdot f)(m) = a \cdot f(m)$ wird V zu einem Vektorraum. Der Nullvektor ist dabei $m \longmapsto 0$.

4.2 Lemma

In einem Vektorraum gilt für alle $\lambda \in K$ und $v \in V$

1. $0 \cdot v = 0$ und $\lambda \cdot 0 = 0$

2. $\lambda \cdot v = 0 \Longrightarrow \lambda = 0$ oder $v = 0$

3. $-v = (-1) \cdot v$

Beweis

1 Es gilt $0 \cdot v = (0 + 0) \cdot v = 0 \cdot v + 0 \cdot v$, d.h. $0 \cdot v$ ist das neutrale Element 0 der abelschen Gruppe V. Analog folgt $\lambda \cdot 0 = 0$ aus $\lambda \cdot 0 = \lambda \cdot (0 + 0) = \lambda \cdot 0 + \lambda \cdot 0$.

2 Sei $\lambda \cdot v = 0$ und $\lambda \neq 0$. Es folgt $0 = \lambda^{-1} \cdot 0 = \lambda^{-1} \cdot (\lambda \cdot v) = (\lambda^{-1} \cdot \lambda) \cdot v = 1 \cdot v = v$.

3 Es gilt $v + (-1) \cdot v = 1 \cdot v + (-1) \cdot v = \big(1 + (-1)\big) \cdot v = 0 \cdot v = 0$, also ist $(-1) \cdot v$ das Inverse $-v$ von v.

4.3 Definition

Eine Teilmenge $U \subseteq V$ eines Vektorraums V heißt Unterraum, wenn $(U, +)$ eine Untergruppe von $(V, +)$ ist und für alle $\lambda \in K$ und $u \in U$ stets $\lambda \cdot U \in U$ gilt.

4.4 Lemma

Eine nichtleere Teilmenge $U \subseteq V$ eines Vektorraums V ist genau dann ein Unterrraum, wenn für alle $\lambda, \mu \in K$ und $u, v \in U$ stets $\lambda \cdot u + \mu \cdot v \in U$ gilt.

Beweis

Sei U ein Unterraum von V. Für $\lambda, \mu \in K$ und $u, v \in U$ gilt dann $\lambda \cdot u, \mu \cdot v \in U$. Da $(U, +)$ eine Gruppe ist, folgt daher $\lambda \cdot u + \mu \cdot v \in U$.

Sei nun $U \subseteq V$ eine nichtleere Teilmenge mit $\lambda \cdot u + \mu \cdot v \in U$ für alle $\lambda, \mu \in K$ und $u, v \in U$. Für $\lambda = 1$ und $\mu = -1$ folgt insbesondere $u - v \in U$ für alle $u, v \in U$ – d.h. $(U, +)$ ist ein Untergruppe von V. Mit $v = 0$ gilt $\lambda \cdot u \in U$ für alle $\lambda \in K$ und $u \in U$.

Bemerkung

Ein Unterraum U eines K-Vektorraums V ist selbst ein K-Vektorraum.

Beispiel

1. Sei $V = K^n$. Dann ist $U = \{(a, \dots, a) \mid a \in K\}$ ein Unterraum. Für $n = 2$ und $K = \mathbb{R}$ ist U eine Winkelhalbierende des Koordinatensystem.
2. Sei $V = \{f : \mathbb{R}^n \longrightarrow \mathbb{R}^m\}$. Dann ist $U = \{f \in V \mid f \text{ stetig}\}$ ein Unterraum.
3. Sei V ein K-Vektorraum und $v \in V$. Dann ist $Kv = \{\lambda \cdot v \mid \lambda \in K\}$ ein Unterraum, da $Kv \neq \emptyset$ sowie $u_1, u_2 \in Kv \Longrightarrow u_1 = \lambda_1 \cdot v$ und $u_2 = \lambda_2 \cdot v \Longrightarrow \mu_1 \cdot (\lambda_1 \cdot v) + \mu_2 \cdot (\lambda_2 \cdot v) = (\mu_1 \cdot \lambda_1 + \mu_2 \cdot \lambda_2) \cdot v \in Kv$.

4.5 Satz

Sei V ein Vektorraum. Dann ist ein Schnitt beliebig vieler Unterräume von V wieder ein Unterraum.

Beweis

Sei $\{U_i \mid i \in I\}$ eine Menge von Unterräumen und $S = \bigcap\limits_{i \in I} U_i$. Man wähle $u, v \in S$ und $\lambda, \mu \in K$ beliebig. Dann gilt $u, v \in U_i \Longrightarrow \lambda \cdot u + \mu \cdot v \in U_i$ für alle $i \in I$, d.h. $\lambda \cdot u + \mu \cdot v \in S$.

4.6 Definition

Sei V ein K-Vektorraum. Dann heißt eine Summe $\sum\limits_{i=1}^{n} \lambda_i \cdot v_i$ mit $\lambda_i \in K$ eine Linearkombination der Vektoren $v_i \in V$.

4.7 Satz / Definition

Sei $M \neq \emptyset$ eine Teilmenge $M \subseteq V$ des Vektorraums V. Dann ist $\langle M \rangle = \{\sum\limits_{i=1}^{n} \lambda_i \cdot v_i \mid 0 < n \in \mathbb{N},\ \lambda_i \in K \text{ und } v_i \in M\}$ der kleinste Unterraum, der M enthält. Man nennt $\langle M \rangle$ das Erzeugnis von M.

Beweis

Offenbar gilt $\langle M \rangle \neq \emptyset$ sowie $\lambda, \mu \in K,\ u, v \in M \Longrightarrow \lambda \cdot u + \mu \cdot v \in M$. Damit ist $\langle M \rangle$ ein Unterraum. Mit $\lambda_j = 1$ und $\lambda_i = 0$ für alle $i \neq j$ gilt $v_j = \sum\limits_{i=1}^{n} \lambda_i \cdot v_i$, also $M \subseteq \langle M \rangle$.

Sei nun U ein Unterraum mit $M \subseteq U$. Wegen Lemma 4.4 liegt jede Linearkombination der Vektoren aus M wieder in U, d.h. $\langle M \rangle \subseteq U$. Damit ist $\langle M \rangle$ der kleinste Unterraum, der M enthält.

4.8 Definition

Sei V ein Vektorraum. Dann ist $U_1 + \ldots + U_n = \langle U_1 \cup \ldots \cup U_n \rangle$ die Summe der Unterräume $U_1, \ldots, U_n$ von V.

Bemerkung

Die Summe $U_1 + \ldots + U_n$ besteht aus allen Elementen der Form $u_1 + \ldots + u_n$ mit $u_i \in U_i$.

Beweis

Ein Element $v \in U_1 + \ldots + U_n$ ist eine Linearkombination $\sum\limits_{i=1}^{m} \lambda_i \cdot v_i$ mit $v_i \in U_1 \cup \ldots \cup U_n$. Es folgt $\sum\limits_{i=1}^{m} \lambda_i \cdot v_i = \sum\limits_{v_i \in U_1} \lambda_i \cdot v_i + \ldots + \sum\limits_{v_i \in U_n} \lambda_i \cdot v_i$. Dabei gilt $\sum\limits_{v_i \in U_j} \lambda_i \cdot v_i = u_j$ für ein $u_j \in U_j$.

4.9 Definition

Sei V ein Vektorraum. Dann heißt eine Teilmenge $M \subseteq V$ mit $\langle M \rangle = V$ ein Erzeugendensystem von V. Ein Erzeugendensystem $M \subseteq V$ heißt minimal, wenn $\langle \widetilde{M} \rangle \subsetneq V$ für alle $\widetilde{M} \subsetneq M$ gilt.

Beispiel

Sei $V = K^2$. Wegen $(a, b) = a \cdot (1, 0) + b \cdot (0, 1)$ für $(a, b) \in V$ ist $V = \langle \{(1, 0), (0, 1)\} \rangle$.

4.10 Definition

Sei V ein Vektorraum und $v_1, \ldots, v_n \in V$. Dann heißen die Vektoren $v_1, \ldots, v_n$ linear abhängig, wenn eine nichttriviale Linearkombination $\sum\limits_{i=1}^{n} \lambda_i \cdot v_i = 0$ existiert. Die Summe $\sum\limits_{i=1}^{n} \lambda_i \cdot v_i$ heißt nichttrivial, wenn es ein $i = 1, \ldots, n$ mit $\lambda_i \neq 0$ gibt. Sind $v_1, \ldots, v_n$ nicht linear abhängig, so heißen sie linear unabhängig.

Eine endliche Teilmenge $\{v_1, \ldots, v_n\} \subseteq V$ heißt linear unabhängig, wenn die Vektoren $v_1, \ldots, v_n$ linear unabhängig sind. Eine beliebige Teilmenge $M \subseteq V$ heißt linear unabhängig, wenn jede endliche Teilmenge von M linear unabhängig ist.

Bemerkung

Jede Teilmenge $M \subseteq V$ eines Vektorraums V mit $0 \in M$ ist wegen $\lambda \cdot 0 = 0$ für alle $\lambda \in K$ linear abhängig.

Beispiel

Sei $V = K^2$ mit $u = (1,0)$, $v = (0,1)$ und $w = (1,1)$. Wegen $0 = a \cdot (1,0) + b \cdot (0,1) = (a,b) \Longrightarrow a = 0 \wedge b = 0$ sind u und v linear unabhängig. Wegen $u + v - w = 0$ sind u, v und w linear abhängig.

4.11 Lemma

Sei M ein Erzeugendensystem des Vektorraums V. Dann sind äquivalent:

1. M ist minimales Erzeugendensystem.
2. M ist linear unabhängig.

Beweis

1 $\Longrightarrow$ 2 Sei M linear abhängig. Daher gibt es verschiedene Vektoren $m_1, \ldots, m_n \in M$ mit $\sum\limits_{i=1}^{n} \lambda_i \, m_i = 0$ und o.B.d.A. $\lambda_1 \neq 0$. Es folgt

$$m_1 = \sum_{i=2}^{n} -\frac{\lambda_i}{\lambda_1} \, m_i,$$

d.h. $m_1 \in \langle M \setminus \{m_1\} \rangle$. Damit ist $\langle M \setminus \{m_1\} \rangle = \langle M \rangle = V$ mit $M \setminus \{m_1\} \subsetneq M$, d.h. M ist kein minimales Erzeugendensystem.

2 $\Longrightarrow$ 1 Sei M kein minimales Erzeugendensystem. Wir betrachten $\widetilde{M} \subsetneq M$ mit $m \in M$ und $m \notin \widetilde{M}$ sowie $\langle \widetilde{M} \rangle = V$. Es folgt insbesondere $m \in \langle \widetilde{M} \rangle$, d.h. es existieren $m_1, \ldots, m_n \in \widetilde{M} \subsetneq M$ mit

$$m = \lambda_1 \, m_1 + \ldots + \lambda_n \, m_n \Longleftrightarrow (-1) \, m + \lambda_1 \, m_1 + \ldots + \lambda_n \, m_n = 0.$$

Daher ist M linear abhängig.

4.12 Lemma

Sei die Teilmenge $M \subseteq V$ des Vektorraums V linear unabhängig und $v \in V$. Dann sind äquivalent:

1. $v \notin \langle M \rangle$

2. $M \cup \{v\}$ ist linear unabhängig.

Beweis

1 $\Longrightarrow$ 2 Sei $M \cup \{v\}$ linear abhängig, d.h. es existiere eine Linearkombination $\lambda\, v + \sum\limits_{i=1}^{n} \lambda_i\, m_i = 0$ mit $m_i \in M$ und $\lambda_j \neq 0$ für ein $1 \leq j \leq n$. Da M linear unabhängig und $\lambda_j \neq 0$ ist, gilt dann $\sum\limits_{i=1}^{n} \lambda_i\, m_i \neq 0$ – also $\lambda \neq 0$. Es folgt

$$v = \sum_{i=1}^{n} -\frac{\lambda_i}{\lambda}\, m_i \in \langle M \rangle.$$

2 $\Longrightarrow$ 1 Sei $v \in \langle M \rangle$, d.h. $v = \sum\limits_{i=1}^{n} \lambda_i\, m_i$ für $m_i \in M$. Dann ist

$$0 = (-1)\, v + \sum_{i=1}^{n} \lambda_i\, m_i,$$

d.h. $M \cup \{v\}$ ist linear abhängig.

4.13 Definition

Ein linear unabhängiges Erzeugendensystem $B \subseteq V$ eines Vektorraums V heißt Basis.

4.14 Satz

Sei V ein Vektorraum und $B \subseteq V$. Dann sind äquivalent:

1. B ist ein minimales Erzeugendensystem von V.

2. B ist eine Basis von V.

3. B ist eine maximale linear unabhängige Teilmenge von V.

4. Jedes Element $v \in V$ hat eine eindeutige Darstellung als Linearkombination von Vektoren aus B.

Beweis

1 $\Longleftrightarrow$ **2** Die Behauptung folgt mit Lemma 4.11 und Definition 4.13.

2 $\Longrightarrow$ **3** Sei B eine linear unabhängige Teilmenge von V, die nicht maximal ist. Dann existiert ein $v \in V$, so dass $B \cup \{v\}$ linear unabhängig sind. Nach Lemma 4.12 ist $v \notin \langle B \rangle$, also $\langle B \rangle \subsetneq V$. Damit ist B kein Erzeugendensystem und somit keine Basis.

3 $\Longrightarrow$ **2** Sei nun B eine maximale linear unabhängige Teilmenge von V. Dann ist $B \cup \{v\}$ für alle $v \in V$ linear abhängig. Nach Lemma 4.12 ist $v \in \langle B \rangle$, d.h. $\langle B \rangle = V$. Daher ist B eine Basis von V.

2 $\Longrightarrow$ **4** Jeder Vektor $v \in V$ ist eine Linearkombination $v = \sum\limits_{i \in I} \lambda_i \, b_i$ von Elementen b_i aus B. Wir betrachten nun eine weitere Darstellung $v = \sum\limits_{i \in J} \mu_i \, b_i$. Setze $\lambda_i = 0$ für $i \in J \setminus I$ und $\mu_i = 0$ für $i \in I \setminus J$. Dann folgt

$$0 = v - v = \sum_{i \in I \cup J} \lambda_i \, b_i - \sum_{i \in I \cup J} \mu_i \, b_i = \sum_{i \in I \cup j} (\lambda_i - \mu_i) \, b_i .$$

Da B linear unabhängig ist, erhält man $\lambda_i - \mu_i = 0 \Longleftrightarrow \lambda_i = \mu_i$ für alle $i \in I \cup J$. Also hat v die eindeutige Darstellung $v = \sum\limits_{i \in I \cup J} \lambda_i \, b_i$.

4 $\Longrightarrow$ **2** Da jeder Vektor $v \in V$ eine Darstellung als Linearkombination von Elementen aus B hat, ist B ein Erzeugendensystem von V.

Seien nun $b_1, \ldots, b_n \in B$ beliebig mit $\sum\limits_{i=1}^{n} \lambda_i \, b_i = 0$. Da die Darstellung $\sum\limits_{i=1}^{n} 0 \cdot b_i = 0 \in V$ eindeutig ist, folgt $\lambda_i = 0$ für alle $1 \leq i \leq n$. Damit ist B linear unabhängig.

4.15 Satz

Jeder endlich erzeugte Vektorraum V besitzt eine Basis.

Beweis

Sei $V = \langle M \rangle$ das Erzeugnis der endlichen Menge M. Dann existiert eine minimale Teilmenge $B \subseteq M$ mit $\langle B \rangle = \langle M \rangle = V$. Nach Satz 4.14 ist dann B eine Basis.

Bemerkung

Mit Hilfe des Zornschen Lemmas kann man zeigen, dass auch unendlich erzeugte Vektorräume stets eine Basis besitzen. Das Zornsche Lemma ist äquivalent zu dem Auswahlaxiom.

Beispiel

1. Sei $0 < n \in \mathbb{N}$ und $e_j = (\lambda_1, \ldots, \lambda_n) \in K^n$ mit $\lambda_j = 1$ und $\lambda_i = 0$ für $i \neq j$. Dann ist $\{e_1, \ldots, e_n\} = \{(1, \ldots, 0), \ldots, (0, \ldots, 1)\}$ die Standardbasis von K^n.

2. Es ist $\{(0, 1), (1, 0)\}$ die Standardbasis von K^2. Eine weitere Basis ist durch $B = \{(1, 0), (1, 1)\}$ gegeben: Wegen $v \in K^2 \Longrightarrow v = (a, b) = (a - b) \cdot (1, 0) + b \cdot (1, 1)$ für $a, b \in K$ ist B ein Erzeugendensystem von K^2 und wegen $(0, 0) = a \cdot (1, 0) + b \cdot (1, 1) = (a + b, b) \Longrightarrow b = 0 \Longrightarrow a = 0$ ist B linear unabhängig.

3. $\{x^i \mid i \in \mathbb{N}\}$ ist eine Basis für den Vektorraum aller reellen Polynome.

4.16 Satz (Austauschsatz von Steinitz)

Sei $B = \{b_1, \ldots, b_n\}$ eine Basis des Vektorraums V. Seien weiter $a_1, \ldots, a_k \in V$ linear unabhängig. Dann gilt $k \leq n$ und für eine geeignete Permutation $\pi \in S_n$ ist $\{a_1, \ldots, a_k, b_{\pi(k+1)}, \ldots, b_{\pi(n)}\}$ eine Basis von V.

Beweis

Wir zeigen die Aussage durch vollständige Induktion über k.

Zunächst untersuchen wir die Menge $\{a_1\}$. Dann gilt offenbar $k \leq n$. Mit $\langle B \rangle = V$ ist $a_1 = \lambda_1 \cdot b_1 + \ldots + \lambda_n \cdot b_n$ für $\lambda_i \in K$. Da $\{a_1\}$ linear unabhängig ist, gilt $a_1 \neq 0$. Daher existiert ein $1 \leq j \leq n$ mit $\lambda_j \neq 0$.

Man betrachte nun $\widetilde{B} = \{a_1, b_1, \ldots, b_{j-1}, b_{j+1}, \ldots, b_n\}$.

Wegen
$$b_j = \frac{1}{\lambda_j} \cdot a_1 - \frac{\lambda_1}{\lambda_j} \cdot b_1 - \ldots - \frac{\lambda_{j-1}}{\lambda_j} \cdot b_{j-1} - \frac{\lambda_{j+1}}{\lambda_j} \cdot b_{j+1} - \ldots - \frac{\lambda_n}{\lambda_j} \cdot b_n$$
gilt $b_j \in \widetilde{B}$, d.h. $\langle \widetilde{B} \rangle = \langle \widetilde{B} \cup \{b_j\} \rangle = \langle B \cup \{a_1\} \rangle = V$.

Sei nun $\mu \cdot a_1 + \mu_1 \cdot b_1 + \ldots + \mu_{j-1} \cdot b_{j-1} + \mu_{j+1} \cdot b_{j+1} + \ldots + \mu_n \cdot b_n = 0$. Mit $a_1 = \sum\limits_{i=1}^{n} \lambda_i \cdot b_i$ folgt

$$\begin{aligned}
0 &= \mu \cdot a_1 + \mu_1 \cdot b_1 + \ldots + \mu_{j-1} \cdot b_{j-1} + \mu_{j+1} \cdot b_{j+1} + \ldots + \mu_n \cdot b_n \\
&= \mu \cdot \left(\sum_{i=1}^{n} \lambda_i \cdot b_i \right) + \mu_1 \cdot b_1 + \ldots + \mu_{j-1} \cdot b_{j-1} + \mu_{j+1} \cdot b_{j+1} + \ldots + \mu_n \cdot b_n \\
&= (\mu \cdot \lambda_1 + \mu_1) \cdot b_1 + \ldots + (\mu \cdot \lambda_{j-1} + \mu_{j-1}) \cdot b_{j-1} + \mu \cdot \lambda_j \cdot b_j \\
&+ (\mu \cdot \lambda_{j+1} + \mu_{j+1}) \cdot b_{j+1} + \ldots + (\mu \cdot \lambda_n + \mu_n) \cdot b_n.
\end{aligned}$$

Da B linear unabhängig ist, folgt $\mu \cdot \lambda_i + \mu_i = 0$ für $i \neq j$ und $\mu \cdot \lambda_j = 0$. Mit $\lambda_j \neq 0$ folgt $\mu = 0$ und damit $\mu_i = 0$ für $i \neq j$.

Insgesamt ist also $\widetilde{B}$ ein linear unabhängiges Erzeugendensystem – d.h. eine Basis – von V.

Nun gelte für jede linear unabhängige Teilmenge $\{a_1, \ldots, a_{k-1}\}$ stets $k-1 \leq n$ und es existiere eine Permutation $\delta \in S_n$, so dass $\{a_1, \ldots, a_{k-1}, b_{\delta(k)}, \ldots, b_{\delta(n)}\}$ eine Basis von V ist. Seien dann $a_1, \ldots, a_k \in V$ – also insbesondere $a_1, \ldots, a_{k-1}$ – linear unabhängig.

Nach Annahme gilt $k-1 \leq n$. Da $a_1, \ldots, a_k \in V$ linear unabhängig sind, ist $\{a_1, \ldots, a_{k-1}\}$ keine maximale linear unabhängige Teilmenge – d.h. keine Basis – von V. Da aber $\{a_1, \ldots, a_{k-1}, b_{\delta(k)}, \ldots, b_{\delta(n)}\}$ eine Basis von V ist, gilt $\left|\{b_{\delta(k)}, \ldots, b_{\delta(n)}\}\right| \geq 1$ – d.h. $k \leq n$.

Wegen $\langle\{a_1, \ldots, a_{k-1}, b_{\delta(k)}, \ldots, b_{\delta(n)}\}\rangle = V$ gibt es Skalare $\lambda_i \in K$ mit $a_k = \lambda_1 \cdot a_1 + \ldots + \lambda_{k-1} \cdot a_{k-1} + \lambda_k \cdot b_{\delta(k)} + \ldots + \lambda_n \cdot b_{\delta(n)}$. Da $a_1, \ldots, a_k \in V$ linear unabhängig sind, gilt $a_k \notin \langle\{a_1, \ldots, a_{k-1}\}\rangle$. Daher existiert ein $k \leq j \leq n$ mit $\lambda_j \neq 0$.

Wir betrachten nun $\widehat{B} = \{a_1, \ldots, a_k, b_{\delta(k)}, \ldots, b_{\delta(j-1)}, b_{\delta(j+1)}, \ldots, b_{\delta(n)}\}$.

Wegen

$$\begin{aligned} b_{\delta(j)} &= \tfrac{1}{\lambda_j} \cdot a_k - \tfrac{\lambda_1}{\lambda_j} \cdot a_1 - \ldots - \tfrac{\lambda_{k-1}}{\lambda_j} \cdot a_{k-1} \\ &- \tfrac{\lambda_k}{\lambda_j} \cdot b_{\delta(k)} - \ldots + \tfrac{\lambda_{j-1}}{\lambda_j} \cdot b_{\delta(j-1)} - \tfrac{\lambda_{j+1}}{\lambda_j} \cdot b_{\delta(j+1)} - \ldots - \tfrac{\lambda_n}{\lambda_j} \cdot b_{\delta(n)} \end{aligned}$$

ist $b_{\delta(j)} \in \langle\widehat{B}\rangle$. Also folgt $\langle\widehat{B}\rangle = \langle\widehat{B} \cup \{b_{\delta(j)}\}\rangle = \langle\{a_1, \ldots, a_{k-1}, b_{\delta(k)}, \ldots, b_{\delta(n)}\} \cup \{a_k\}\rangle = V$.

Sei weiter $\mu_1 \cdot a_1 + \ldots + \mu_{k-1} \cdot a_{k-1} + \mu \cdot a_k + \mu_k \cdot b_{\delta(k)} + \ldots + \mu_{j-1} \cdot b_{\delta(j-1)} + \mu_{j+1} \cdot b_{\delta(j+1)} + \ldots + \mu_n \cdot b_{\delta(n)} = 0$. Mit $a_k = \sum\limits_{i=1}^{k-1} \lambda_i \cdot a_i + \sum\limits_{i=k}^{n} \lambda_i \cdot b_{\delta(i)}$ folgt

$$\begin{aligned} 0 &= \mu_1 \cdot a_1 + \ldots + \mu_{k-1} \cdot a_{k-1} + \mu \cdot a_k + \mu_k \cdot b_{\delta(k)} + \ldots + \mu_{j-1} \cdot b_{\delta(j-1)} \\ &+ \mu_{j+1} \cdot b_{\delta(j+1)} + \ldots + \mu_n \cdot b_{\delta(n)} \\ &= \mu_1 \cdot a_1 + \ldots + \mu_{k-1} \cdot a_{k-1} + \mu \cdot \left(\sum_{i=1}^{k-1} \lambda_i \cdot a_i + \sum_{i=k}^{n} \lambda_i \cdot b_{\delta(i)}\right) \\ &+ \mu_k \cdot b_{\delta(k)} + \ldots + \mu_{j-1} \cdot b_{\delta(j-1)} + \mu_{j+1} \cdot b_{\delta(j+1)} + \ldots + \mu_n \cdot b_{\delta(n)} \\ &= (\mu_1 + \mu \cdot \lambda_1) \cdot a_1 + \ldots + (\mu_{k-1} + \mu \cdot \lambda_{k-1}) \cdot a_{k-1} \\ &+ (\mu_k + \mu \cdot \lambda_k) \cdot b_{\delta(k)} + \ldots + (\mu_{j-1} + \mu \cdot \lambda_{j-1}) \cdot b_{\delta(j-1)} + \mu \cdot \lambda_j \cdot b_{\delta(j)} \\ &+ (\mu_{j+1} + \mu \cdot \lambda_{j+1}) \cdot b_{\delta(j+1)} + \ldots + (\mu_n + \mu \cdot \lambda_n) \cdot b_{\delta(n)}. \end{aligned}$$

Da nun $\{a_1, \ldots, a_{k-1}, b_{\delta(k)}, \ldots, b_{\delta(n)}\}$ linear unabhängig ist, folgt $\mu_i + \mu \cdot \lambda_i = 0$ für $i \neq j$ und $\mu \cdot \lambda_j = 0$. Mit $\lambda_j \neq 0$ folgt $\mu = 0$ und damit $\mu_i = 0$ für $i \neq j$.

Insgesamt ist $\widehat{B}$ eine Basis von V. Setzt man dann $\pi(i) = \delta(i-1)$ für $k+1 \leq i \leq j$ und $\pi(i) = \delta(i)$ für $i > j$, so erhält man $\widehat{B} = \{a_1, \dots, a_k, b_{\pi(k+1)}, \dots, b_{\pi(n)}\}$.

4.17 Korollar

Je zwei endliche Basen eines Vektorraums haben die gleiche Mächtigkeit.

Beweis

Sei $A = \{a_1, \dots, a_k\}$ und $C = \{b_1, \dots, b_n\}$ Basen des Vektorraums V. Da A und B dann linear unabhängig sind, folgt mit Satz 4.16 stets $k \leq n$ und $n \leq k$. Daher gilt $k = n$.

4.18 Definition

Sei $B = \{b_1, \dots, b_n\}$ eine Basis des Vektorraums V. Dann hängt n nur von V ab und heißt Dimension von V. Man schreibt $\dim V = n$.

Hat V keine endliche Basis, so schreibt man $\dim V = \infty$.

Beispiel

1. Die Menge $\{0\}$ ist linear abhängig. Daher gilt $\dim \{0\} = 0$.
2. Sei K ein Körper. Dann ist $\dim K^n = n$.
3. Sei V die Menge der reellen Polynome. Dann gilt $\dim V = \infty$.

4.19 Lemma

Sei $\dim V < \infty$ und $U \subseteq V$ ein Unterraum. Dann gilt $\dim U \leq \dim V$ mit $\dim U = \dim V \iff U = V$.

Beweis

Da U selbst ein Vektorraum ist, besitzt U eine Basis B. Dann ist B eine linear unabhängige Teilmenge von V und nach Satz 4.16 gilt $\dim U = |B| \leq \dim V$.

Für $\dim U = \dim V$ ist B schon eine Basis von V, d.h. $U = \langle B \rangle = V$. Für $U = V$ gilt offenbar $\dim U = \dim V$.

4.20 Satz (Dimensionssatz für Unterräume)

Seien U und W endlich-dimensionale Unterräume eines beliebigen Vektorraums V. Dann gilt $\dim U + \dim W = \dim(U \cap W) + \dim(U + W)$.

Beweis

Nach Satz 4.5 ist $U \cap W$ ein Unterraum. Sei dann $A = \{a_1, \ldots, a_m\}$ eine Basis von $U \cap W$. Als Teilmenge $U \cap W \subseteq U$ ist $U \cap W$ ein Unterraum von U. Daher lässt sich A nach Satz 4.16 zu einer Basis $\{a_1, \ldots, a_m, u_1, \ldots, u_r\}$ von U ergänzen. Analog ist $\{a_1, \ldots, a_m, w_1, \ldots, w_s\}$ eine Basis von W.

Nun untersuchen wir $B = \{a_1, \ldots, a_m, u_1, \ldots, u_r, w_1, \ldots, w_s\}$. Offenbar gilt $v \in \langle B \rangle \iff v = \sum_{i=1}^{m} \lambda_i \; a_i + \sum_{i=1}^{r} \mu_i \; u_i + \sum_{i=1}^{s} \sigma_i \; w_i \iff v \in U + W$, also $\langle B \rangle = U + W$.

Sei nun

$$(*) \qquad \sum_{i=1}^{m} \alpha_i \; a_i + \sum_{i=1}^{r} \beta_i \; u_i + \sum_{i=1}^{s} \gamma_i \; w_i = 0$$

für Skalare $\alpha_i, \beta_i, \gamma_i \in K$. Setze

$$(**) \qquad v = \sum_{i=1}^{m} \alpha_i \; a_i + \sum_{i=1}^{r} \beta_i \; u_i,$$

d.h. $v \in U$. Dann folgt aus $(*)$ weiter

$$v = -\sum_{i=1}^{s} \gamma_i \; w_i,$$

d.h. $v \in W$ und daher $v \in U \cap W$. Damit ist v eine Linearkombination der Basisvektoren $a_1, \ldots, a_m$ von $U \cap W$. Da aber eine Basisdarstellung eindeutig ist, folgt aus $(**)$ somit $\beta_i = 0$ für $1 \leq i \leq r$.

Aus $(*)$ ergibt sich daher

$$\sum_{i=1}^{m} \alpha_i \; a_i + \sum_{i=1}^{s} \gamma_i \; w_i = 0.$$

Dies ist aber eine Linearkombination der Basisvektoren von W, d.h. $\alpha_i = 0$ für $1 \leq i \leq m$ und $\gamma_i = 0$ für $1 \leq i \leq s$.

Insgesamt ist also B eine Basis von $U + W$ und es folgt $\dim U + \dim W = m + r + m + s = \dim(U \cap W) + \dim(U + W)$.

5 Koordinaten und Matrizen

5.1 Definition

Seien V und W Vektorräume über K. Eine Abbildung $\varphi : V \longrightarrow W$ heißt Homomorphismus oder lineare Abbildung, wenn gilt:

1. $\varphi(u+v) = \varphi(u) + \varphi(v)$ für alle $u, v \in V$
2. $\varphi(\lambda \cdot v) = \lambda \cdot \varphi(v)$ für alle $v \in V$ und $\lambda \in K$

Bemerkung

1. Eine lineare Abbildung $\varphi : V \longrightarrow W$ ist wegen $\varphi(\lambda \cdot v) = \lambda \cdot \varphi(v)$ nur für Vektorräume über dem gleichen Skalarenkörper definiert.
2. Für eine lineare Abbildung gilt $\varphi(0) = \varphi(0 \cdot v) = 0 \cdot \varphi(v) = 0$.
3. Die Bezeichnungen für lineare Abbildungen sind äquivalent zu den Bezeichnungen für Gruppen- und Ringhomomorphismen.

Beispiel

1. $\varphi : v \in V \longmapsto 0 \in W$ ist linear
2. $\varphi : v \in V \longmapsto c \cdot v \in V$ für ein festes $c \in K$ ist wegen
   (a) $\varphi(v+w) = c(v+w) = cv + cw = \varphi(v) + \varphi(w)$
   (b) $\varphi(\lambda v) = c(\lambda v) = \lambda(cv) = \lambda\, \varphi(v)$

   linear.
3. Für $V = \{f : \mathbb{R} \longrightarrow \mathbb{R}\}$ ist $\varphi : f \in V \longmapsto f(0) \in \mathbb{R}$ linear.

Bemerkung

Wir betrachten nun eine Basis $B = \{v_1, \ldots, v_n\}$ des Vektorraums V mit festgewählter Reihenfolge $v_1, \ldots, v_n$.

5.2 Definition

Sei $v_1, \ldots, v_n$ eine Basis des Vektorraums V. Für alle $v \in V$ gibt es eindeutig bestimmte Skalare $\lambda_1, \ldots, \lambda_n$ mit $v = \sum_{i=1}^{n} \lambda_i v_i$. Man nennt $\lambda_1, \ldots, \lambda_n$ die Koordinaten und $(\lambda_1, \ldots, \lambda_n) \in K^n$ den Koordinatenvektor von v.

Beispiel

Sei $V = \mathbb{R}^2$ mit der Basis $v_1 = (1,0)$ und $v_2 = (1,1)$ gegeben. Der Vektor $(a,b) \in V$ hat dann wegen $(a,b) = (a-b)\,v_1 + b\,v_2$ den Koordinatenvektor $(a-b, b)$.

5.3 Definition / Satz

Sei $v_1, \ldots, v_n$ eine Basis des K-Vektorraums V. Die Abbildung $\varphi : V \longrightarrow K^n$ sei definiert durch $\varphi(v) = (\lambda_1, \ldots, \lambda_n)$ für $v = \sum_{i=1}^{n} \lambda_i v_i$. Dann heißt φ Koordinatenabbildung und ist ein Isomorphismus.

Beweis

Da die Basisdarstellung eines Vektors $v \in V$ eindeutig ist, ist φ wohldefiniert. Sei dann $v = \sum \lambda_i v_i$ und $w = \sum \mu_i v_i$.

Es folgt

$$\begin{aligned} \varphi(v+w) &= \varphi(\textstyle\sum \lambda_i v_i + \sum \mu_i v_i) &&= \varphi(\textstyle\sum (\lambda_i + \mu_i) v_i) \\ &= (\lambda_1 + \mu_1, \ldots, \lambda_n + \mu_n) &&= (\lambda_1, \ldots, \lambda_n) + (\mu_1, \ldots, \mu_n) \\ &= \varphi(\textstyle\sum \lambda_i v_i) + \varphi(\sum \mu_i v_i) &&= \varphi(v) + \varphi(w) \end{aligned}$$

und

$$\begin{aligned} \varphi(\lambda w) &= \varphi(\lambda \cdot \textstyle\sum \mu_i v_i) &&= \varphi(\textstyle\sum (\lambda \mu_i) v_i) \\ &= (\lambda\mu_1, \ldots, \lambda\mu_n) &&= \lambda \cdot (\mu_1, \ldots, \mu_n) \\ &= \lambda \varphi(\textstyle\sum \mu_i v_i) &&= \lambda \varphi(w) \end{aligned}$$

Die Bijektivität ist offensichtlich.

Beispiel

Sei V der Vektorraum der reellen Polynome $p \in \mathbb{R}[x]$ mit grad $p \leq 2$. Dann ist $v_1 = x^0$, $v_2 = x^1$ und $v_3 = x^2$ eine Basis. Dann gilt für die Koordinatenabbildung $\varphi(17x^2+3x-5) = (-5, 3, 17)$.

5.4 Satz

Seien $v_1, \ldots, v_n$ und $\widetilde{v}_1, \ldots, \widetilde{v}_n$ Basen eines Vektorraums V mit $\widetilde{v}_k = \sum\limits_{i=1}^{n} a_{ik} v_i$ für $1 \leq k \leq n$. Für $v \in V$ seien $(\lambda_1, \ldots, \lambda_n)$ und $(\widetilde{\lambda}_1, \ldots, \widetilde{\lambda}_n)$ die Koordinatenvektoren bzgl. der verschiedenen Basen. Dann gilt $\lambda_i = \sum\limits_{k=1}^{n} a_{ik} \widetilde{\lambda}_k$ für $1 \leq i \leq n$.

Beweis

Es gilt $v = \sum\limits_{i=1}^{n} \lambda_i v_i$ und $v = \sum\limits_{k=1}^{n} \widetilde{\lambda}_k \widetilde{v}_k$. Mit $\widetilde{v}_k = \sum\limits_{i=1}^{n} a_{ik} v_i$ folgt

$$
\begin{aligned}
\sum_{i=1}^{n} \lambda_i v_i = v &= \sum_{k=1}^{n} \widetilde{\lambda}_k \widetilde{v}_k &&= \sum_{k=1}^{n} \widetilde{\lambda}_k \left(\sum_{i=1}^{n} a_{ik} v_i \right) \\
&= \sum_{k=1}^{n} \sum_{i=1}^{n} \widetilde{\lambda}_k a_{ik} v_i &&= \sum_{i=1}^{n} \sum_{k=1}^{n} \widetilde{\lambda}_k a_{ik} v_i \\
&= \sum_{i=1}^{n} \left(\sum_{k=1}^{n} \widetilde{\lambda}_k a_{ik} \right) v_i.
\end{aligned}
$$

Da die Darstellung von v bzgl. der Basis $v_1, \ldots, v_n$ eindeutig ist, liefert ein Koeffizientenvergleich $\lambda_i = \sum\limits_{k=1}^{n} a_{ik} \widetilde{\lambda}_k$.

5.5 Definition

Sei R ein Ring und $m, n \in \mathbb{N}^+$. Dann ist eine $(m \times n)$-Matrix A eine Abbildung $(i, j) \in \{1, \ldots, m\} \times \{1, \ldots, n\} \longrightarrow a_{ij} \in R$. Man schreibt

$$
A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.
$$

Für $m = n$ heißt A quadratisch. Die Transponierte A^t von A ist eine $(n \times m)$-Matrix

$$
A^t = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{pmatrix}.
$$

Für $m = n$ ist eine Diagonalmatrix durch

$$A = \begin{pmatrix} a_{11} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_{nn} \end{pmatrix} = \begin{pmatrix} a_{11} & & \\ & \ddots & \\ & & a_{nn} \end{pmatrix}$$

definiert. In diesem Fall wird A für $a_{11} = \ldots = a_{nn} = 1$ als Einheitsmatrix 1_n bezeichnet.

Bemerkung

Im Folgenden beschreiben wir die Koordinaten von $v = \sum_{i=1}^{n} \lambda_i v_i$ durch einen Spaltenvektor

$$\varphi(v) = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}.$$

Bemerkung

Sei $v_1, \ldots, v_n$ eine Basis des Vektorraums V und seien $\widetilde{v}_k = \sum_{i=1}^{n} a_k v_i$ für $1 \leq k \leq n$ weitere n Vektoren. Dann bilden die Vektoren $\widetilde{v}_1, \ldots, \widetilde{v}_n$ genau dann eine Basis, wenn sie linear unabhängig sind.

Da $\varphi : V \longrightarrow K^n$ ein Isomorphismus ist, gilt

$$\sum_{i=k}^{n} \lambda_k \widetilde{v}_k = 0 \Longleftrightarrow \sum_{i=k}^{n} \lambda_k \varphi(\widetilde{v}_k) = \varphi(\sum_{k=1}^{n} \lambda_k \widetilde{v}_k) = \varphi(0) = 0.$$

Daher sind die $\widetilde{v}_k$ genau dann linear unabhängig, wenn die Spaltenvektoren

$$\varphi(\widetilde{v}_k) = \begin{pmatrix} a_{1k} \\ \vdots \\ a_{nk} \end{pmatrix}$$

linear unabhängig sind. Es ist also zu entscheiden, ob die Spalten der Matrix

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$

linear unabhängig sind.

5.6 Definition

Sei A eine $(m \times n)$-Matrix über einem Körper K. Der Rang von A ist die Mächtigkeit einer maximalen Menge linear unabhängiger Spalten von A. Man schreibt rang A.

Bemerkung

Da die Spalten einer $(m \times n)$-Matrix A eine Teilmenge $M \subseteq K^m$ sind, hängt der rang A von dem gewählten Skalarenkörper ab.

5.7 Lemma

Der Rang einer Matrix A ist die Dimension des von ihren Spalten erzeugten Unterraums von K^m.

Beweis

Die Spalten einer $(m \times n)$-Matrix über einem Körper K bilden einer Teilmenge $M \subseteq K^m$. Sei nun S eine maximale linear unabhängig Teilmenge $S \subseteq M$. Dann ist S auch eine maximale linear unabhängige Teilmenge von $\langle M \rangle$, d.h. eine Basis von $\langle M \rangle$. Daher gilt $\dim\langle M \rangle = |S|$.

5.8 Lemma

Sei $M \subseteq V$ eine Menge von Vektoren in einem endlich-dimensionalen Vektorraum V. Die Menge $\widetilde{M}$ entstehe durch Anwendung einer der folgenden Operationen:

1. Man ersetzt ein $v \in M$ durch λv für $0 \neq \lambda \in K$.

2. Sei $u, v \in M$. Man ersetzt u durch $u + \lambda v$ für $\lambda \in K$.

Dann gilt $\langle M \rangle = \langle \widetilde{M} \rangle$.

Beweis

1 Da K ein Körper und $\lambda \neq 0$ ist, existiert $\frac{1}{\lambda}$. Es folgt $v = \frac{1}{\lambda}\lambda v \in \langle \widetilde{M} \rangle$, d.h. $\langle M \rangle \subseteq \langle \widetilde{M} \rangle$. Wegen $\lambda v \in \langle M \rangle$ gilt aber auch $\langle \widetilde{M} \rangle \subseteq \langle M \rangle$.

2 Analog zu 1 gilt $u, v \in M \Longrightarrow u + \lambda v \in \langle M \rangle \Longrightarrow \langle \widetilde{M} \rangle \subseteq \langle M \rangle$ und $u + \lambda v, v \in \widetilde{M} \Longrightarrow u = u + \lambda v - \lambda v \in \langle \widetilde{M} \rangle \Longrightarrow \langle M \rangle \subseteq \langle \widetilde{M} \rangle$.

5.9 Satz (elementare Spaltenoperationen)

Der Rang einer Matrix ändert sich nicht, wenn man folgende Operationen auf die Matrix anwendet:

1. Man multipliziert eine Spalte mit $0 \neq \lambda \in K$.

2. Seien u und v Spalten. Man ersetzt u durch $u + \lambda v$ für $\lambda \in K$.

3. Man vertauscht zwei Spalten.

Beweis

Sei $M \subseteq K^m$ die Menge der Spalten der $(m \times n)$-Matrix A. Dann ist $\operatorname{rang} A = \dim\langle M \rangle$. Nach Lemma 5.8 folgt 1 und 2. Da die Elemente einer Menge unabhängig von der Reihenfolge sind, gilt 3.

5.10 Definition / Bemerkung

Unter dem Zeilenrang einer Matrix A versteht man die maximale Anzahl linear unabhängiger Zeilen. Der Zeilenrang von A entspricht daher $\operatorname{rang} A^t$, d.h. Satz 5.9 gilt sinngemäß für elementare Zeilenoperationen.

Beispiel

Wir untersuchen den Zeilenrang von

$$A = \begin{pmatrix} 1 & 3 & -4 & 3 \\ 3 & 9 & -2 & -11 \\ 4 & 12 & -6 & -6 \\ 2 & 6 & 2 & -10 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 3 & -4 & 3 \\ & & 10 & -20 \\ & & 10 & -18 \\ & & 10 & -16 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 1 & 3 & -4 & 3 \\ & & 10 & -20 \\ & & & 2 \\ & & & 4 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 3 & -4 & 3 \\ & & 10 & -20 \\ & & & 2 \\ & & & \end{pmatrix}.$$

Es gilt also $\operatorname{rang} A = 3$.

5.11 Definition

Sei $A = (a_{ij})$ für $1 \leq i \leq m$ und $1 \leq j \leq n$ eine $(m \times n)$-Matrix. Für $1 \leq i \leq m$ sei k_i maximal mit $a_{i1} = \cdots = a_{ik_i} = 0$. Setze $k_i = 0$, falls für alle Einträge der i-ten Zeile $a_{ij} = 0$ gilt. Es gelte nun $k_i < k_{i+1}$ für $k_i < n$ und $k_i = k_{i+1}$ für $k_i = n$. Dann heißt A in Zeilenstufenform.

5.12 Satz (Gauß-Algorithmus)

Jede Matrix lässt sich durch elementare Zeilenumformungen auf Zeilenstufenform bringen.

Beweis

Sei die Matrix A gegeben. Wir unterscheiden nun 2 Fälle:

1 In der ersten Spalte kommt ein von 0 verschiedenes Element vor.

$$\begin{pmatrix} 0 & \cdots \\ a_{21} & \cdots \\ a_{31} & \cdots \\ \vdots & \ddots \\ a_{m1} & \cdots \end{pmatrix}$$

Durch Vertauschung entsprechender Zeilen bringen wir dieses Element in die linke obere Ecke der Matrix.

$$\begin{pmatrix} a_{21} & \cdots \\ 0 & \cdots \\ a_{31} & \cdots \\ \vdots & \ddots \\ a_{m1} & \cdots \end{pmatrix}$$

Durch Substraktion geeigneter Vielfacher der ersten Zeilen von den anderen Zeilen erreicht man, dass in der ersten Spalte alle Einträge außer dem obersten gleich 0 sind.

$$\begin{pmatrix} a_{21} & \cdots \\ 0 & \cdots \\ 0 & \cdots \\ \vdots & \ddots \\ 0 & \cdots \end{pmatrix}$$

Dann streichen wir die erste Zeile sowie die erste Spalte und beginnen erneut.

2 In der ersten Spalte sind alle Einträge gleich 0. Dann streichen wir die erste Spalte und beginnen erneut.

5.13 Satz

Die Matrix A sei durch elementare Zeilenumformungen auf Zeilenstufenform gebracht. Dann ist der Zeilenrang von A die Anzahl der vom Nullvektor verschiedenen Zeilen.

Beweis

Sei o.B.d.A.

$$A = \begin{pmatrix} a & b & c & d \\ & & e & f \\ & & & g \\ & & & \end{pmatrix}.$$

Wegen $0 = \alpha \cdot (a, b, c, d) + \beta \cdot (0, 0, e, f) + \gamma \cdot (0, 0, 0, g) \Longrightarrow \alpha = 0 \Longrightarrow \beta = 0 \Longrightarrow \gamma = 0$ sind die ersten drei Zeilen linear unabhängig. Da die vierte Zeile der Nullvektor ist, ist dies die maximale Anzahl linear unabhängiger Zeilen.

5.14 Satz

Elementare Zeilenoperationen ändern nicht den Spaltenrang einer Matrix und elementare Spaltenoperationen ändern nicht den Zeilenrang einer Matrix.

Beweis

Es genügt für eine Matrix A die erste Aussage zu zeigen. Die zweite Aussage folgt aus der Betrachtung von A^t. Sei nun o.B.d.A.

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

Der Spaltenrang von A ändert sich genau nicht, wenn die lineare Unabhängigkiet bzw. lineare Abhängigkeit der Spalten nicht beeinflusst wird. Dabei sind die Spalten

$$\begin{pmatrix} a \\ c \end{pmatrix} \text{ und } \begin{pmatrix} b \\ d \end{pmatrix}$$

genau dann linear abhängig, wenn es ein $(0, 0) \neq (x, y) \in K^2$ mit

$$x \cdot \begin{pmatrix} a \\ c \end{pmatrix} + y \cdot \begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

gibt. Dies entspricht dem Gleichungssystem $(*)$

$$\begin{array}{ccccccc} x & a & + & y & b & = & 0 \\ x & c & + & y & d & = & 0 \end{array}$$

Die Behauptung folgt, da $(*)$ äquivalent zu

1.
$$\begin{array}{ccccccc} x & c & + & y & d & = & 0 \\ x & a & + & y & b & = & 0 \end{array}$$

2.
$$\begin{array}{ccccccccc} x & \lambda & a & + & y & \lambda & b & = & 0 \\ x & & c & + & y & & d & = & 0 \end{array}$$

3.
$$\begin{array}{ccccccccccccccc} x & & & & a & + & y & & & & b & = & 0 \\ x & (\lambda & a & + & c) & + & y & (\lambda & b & + & d) & = & 0 \end{array}$$

ist.

5.15 Satz

Durch eine Folge geeigneter elementarer Zeilen- und Spaltenoperationen lässt sich jede Matrix auf die Form
$$R = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & & \\ \end{pmatrix}$$
bringen. Für $R = (a_{ij})$ mit $1 \leq i \leq m$ und $1 \leq j \leq n$ existiert dann ein $r < m$ und $r < n$, so dass $a_{ii} = 1$ für $1 \leq i \leq r$ und sonst $a_{ij} = 0$ gilt.

Beweis

Sei eine $(m \times n)$-Matrix gegeben. Durch elementare Zeilenoperationen erhält man eine Zeilenstufenform.
$$\begin{pmatrix} & a_{12} & \cdots & & & & \\ & & & a_{24} & \cdots & & \\ & & & & a_{35} & \cdots & \\ & & & & & \ddots & \end{pmatrix}$$
Durch Multiplikation der Zeilen mit geeigneter Faktoren erreicht man, dass jeweils der erste von 0 verschiedene Eintrag 1 ist.
$$\begin{pmatrix} & 1 & \cdots & & & & \\ & & & 1 & \cdots & & \\ & & & & 1 & \cdots & \\ & & & & & \ddots & \end{pmatrix}$$

Sei j die Position dieser 1 in der ersten Zeile. Durch Addition geeigneter Vielfacher der j-ten Spalte zu den Spalten an der Postion $i > j$ erreicht man, dass in der ersten Zeile alle Einträge an einer Position $i \neq j$ gleich 0 sind. Analog verfährt man sukzessive mit den folgenden Zeilen.

$$\begin{pmatrix} & 1 & & & & & \\ & & & 1 & & & \\ & & & & 1 & & \\ & & & & & \ddots & \end{pmatrix}$$

Durch Vertauschung geeigneter Spalten erhält man die gewünschte Form.

$$\begin{pmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \\ & & & \ddots & & & \\ & & & & & & \end{pmatrix}$$

Beispiel

$$\begin{pmatrix} 1 & 3 & -4 & 3 \\ 3 & 9 & -2 & -11 \\ 4 & 12 & -6 & -6 \\ 2 & 6 & 2 & -10 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 3 & -4 & 3 \\ & & 10 & -20 \\ & & & 2 \\ & & & \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 3 & -4 & 3 \\ & & 1 & -2 \\ & & & 1 \\ & & & \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 1 & & & \\ & & 1 & \\ & & & 1 \\ & & & \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & \end{pmatrix}$$

5.16 Korollar

Der Zeilen- und Spaltenrang einer Matrix stimmt überein.

Beweis

Nach Satz 5.14 lassen die Operationen in Satz 5.15 Zeilen- und Spaltenrang einer Matrix unverändert. Satz 5.15 liefert aber eine Matrix, in der offensichtlich Zeilen- und Spaltenrang übereinstimmen.

6 Matrizenraum und Matrizenring

6.1 Definition

Die Menge aller $(m \times n)$-Matrizen über einem Ring R bezeichnet man mit $R^{m \times n}$ oder $M_{m \times n}(R)$. Weitere Schreibweisen sind $Mat_{m,n}(R)$ und $M(m,n,R)$.

6.2 Definition / Lemma

Sei K ein Körper. Dann definiert man auf $M = M_{m \times n}(K)$ eine Addition durch $(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$, so dass $(M, +)$ ein abelsche Gruppe bildet. Durch $\lambda \cdot (a_{ij}) = (\lambda \cdot a_{ij})$ wird M zu einem K-Vektorraum mit $\dim M = m \cdot n$.

Beweis

Da die Addition komponentenweise definiert ist, folgen die Gruppenaxiome aus den Eigenschaften von K. Analog zeigt man, dass M einen Vektorraum bildet. Sei dann

$$B(x,y) = \begin{pmatrix} & & \\ & & \\ & 1 & \\ & & \end{pmatrix} \in M_{m \times n}(K)$$

eine Matrix mit $b_{xy} = 1$ und $b_{ij} = 0$ sonst. Da nun $B = \{B(x,y) \mid 1 \leq x \leq m \wedge 1 \leq y \leq n\}$ eine Basis von M bildet, folgt $\dim M = |B| = m \cdot n$.

6.3 Definition

Sei $(a_{ik}) \in M_{m \times n}(K)$ eine $(m \times n)$-Matrix und $(b_{kj}) \in M_{n \times p}(K)$ eine $(n \times p)$-Matrix. Dann ist ein Produkt $(a_{ik}) \cdot (b_{kj}) = (c_{ij}) \in M_{m \times p}(K)$ durch

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

definiert.

Beispiel

Es gilt

$$\begin{pmatrix} 1 & 2 & 4 \\ 1 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 1 & 1 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 16 \\ 1 & 8 \end{pmatrix}$$

mit etwa

$$\begin{pmatrix} 1 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = 1 \cdot 1 + 0 \cdot 1 + 2 \cdot 0 = 1.$$

6.4 Satz

Für das Matrixprodukt gilt:

1. $(\lambda A)B = A(\lambda B) = \lambda(AB)$ für $\lambda \in K$
2. $A(B + C) = AB + AC$ und $(A + B)C = AC + BC$
3. $(AB)C = A(BC)$
4. $(AB)^t = B^t A^t$

Beweis

1 Sei $A = (a_{ik}) \in K^{m\times n}$, $B = (b_{kj}) \in K^{n\times p}$ und $\lambda \in K$. Dann gilt

$$\begin{aligned} (\lambda A)B &= \big(\lambda \cdot (a_{ik})\big) \cdot (b_{kj}) &&= (\lambda \cdot a_{ik}) \cdot (b_{kj}) \\ &= \big(\sum_{k=1}^{n} (\lambda \cdot a_{ik}) b_{kj}\big) &&= (\lambda \cdot \sum_{k=1}^{n} a_{ik} b_{kj}) \\ &= \lambda \cdot (\sum_{k=1}^{n} a_{ik} b_{kj}) &&= \lambda \cdot (AB) \end{aligned}$$

und analog $A(\lambda B) = \lambda(AB)$.

2 Sei $A = (a_{ik}) \in K^{m\times n}$ und $B = (b_{kj}), C = (c_{kj}) \in K^{n\times p}$. Dann folgt

$$\begin{aligned} A(B + C) &= (a_{ik}) \cdot \big((b_{kj}) + (c_{kj})\big) &&= (a_{ik}) \cdot (b_{kj} + c_{kj}) \\ &= \big(\sum_{k=1}^{n} a_{ik}(b_{kj} + c_{kj})\big) &&= (\sum_{k=1}^{n} a_{ik} b_{kj} + a_{ik} c_{kj}) \\ &= (\sum_{k=1}^{n} a_{ik} b_{kj}) + (\sum_{k=1}^{n} a_{ik} c_{kj}) &&= AB + AC. \end{aligned}$$

Analog gilt $(A+B)C = AC + BC$.

3 Sei $A = (a_{ik}) \in K^{m\times n}$, $B = (b_{kj}) \in K^{n\times p}$ und $C = (c_{jl}) \in K^{p\times r}$. Dann folgt

$$\begin{aligned}
(AB)C &= (\sum_{k=1}^{n} a_{ik}b_{kj})(c_{jl}) &&= \big(\sum_{j=1}^{p}(\sum_{k=1}^{n} a_{ik}b_{kj})c_{jl}\big)\\
&= (\sum_{j=1}^{p}\sum_{k=1}^{n} a_{ik}b_{kj}c_{jl}) &&= (\sum_{k=1}^{n}\sum_{j=1}^{p} a_{ik}b_{kj}c_{jl})\\
&= \big(\sum_{k=1}^{n} a_{ik}(\sum_{j=1}^{p} b_{kj}c_{jl})\big) &&= (a_{ik})(\sum_{j=1}^{p} b_{kj}c_{jl})\\
&= A(BC).
\end{aligned}$$

4 Sei $A = (a_{ik}) \in K^{m\times n}$ und $B = (b_{kj}) \in K^{n\times p}$. Dann ist $A^t = (\widetilde{a}_{ki}) \in K^{n\times m}$ und $B^t = (\widetilde{b}_{jk}) \in K^{p\times n}$ mit $\widetilde{a}_{ki} = a_{ik}$ und $\widetilde{b}_{jk} = b_{kj}$.

Sei weiter $AB = (c_{ij}) \in K^{m\times p}$ und $B^tA^t = (d_{ji}) \in K^{p\times m}$ – d.h. es ist $(AB)^t = B^tA^t$ genau dann, wenn $c_{ij} = d_{ji}$ für alle $1 \le i \le m$ und $1 \le j \le p$ gilt. Es folgt

$$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} = \sum_{k=1}^{n} \widetilde{a}_{ki}\widetilde{b}_{jk} = \sum_{k=1}^{n} \widetilde{b}_{jk}\widetilde{a}_{ki} = d_{ji}.$$

6.5 Korollar

Sei K ein Körper. Dann bilden die quadratischen Matrizen $A \in M = M_{n\times n}(K)$ einen Ring, der für $n \ge 2$ nicht kommutativ ist.

Beweis

Nach Lemma 6.2 ist $(M, +)$ eine abelsche Gruppe. Das Matrixprodukt ist weiter für alle quadratischen Matrizen wohldefiniert. Dabei ist die Einheitsmatrix wegen

$$1_n \cdot A = (\delta_{ij}) \cdot (a_{ij}) = (\sum_{i=1}^{n} \delta_{ik}a_{kj}) = (a_{ij}) = A$$

das neutrale Element. Die weiteren Ringeigenschaften folgen aus Satz 6.4.

Für $n \ge 2$ existieren Matrizen $A = (a_{ij}), B = (b_{ij}) \in K^{n\times n}$ mit $a_{12} = b_{21} = 1$ und sonst $a_{ij} = 0$ bzw. $b_{ij} = 0$. Es folgt

$$AB = \begin{pmatrix} 1 & & \\ & & \\ & & \end{pmatrix} \ne \begin{pmatrix} & & \\ & 1 & \\ & & \end{pmatrix} = BA.$$

6.6 Definition

Eine Matrix $A \in M_{n\times n}(K)$ heißt invertierbar, wenn eine Matrix $B \in M_{n\times n}(K)$ mit $AB = 1_n$ existiert. Man schreibt dann $B = A^{-1}$.

7 Lineare Abbildungen und Matrizen

Bemerkung

Seien V und W Vektorräume mit $V \neq \{0\}$ und sei $\varphi : V \longrightarrow W$ eine lineare Abbildung. Sei weiter B eine Basis von V. Dann ist jeder Vektor $v \in V$ eine eindeutige Linearkombination $v = \sum\limits_{i=1}^{n} \lambda_i b_i$ von Vektoren b_i aus B, d.h. es gilt $\varphi(v) = \sum\limits_{i=1}^{n} \lambda_i \varphi(b_i)$. Daher gilt:

1. Eine lineare Abbildung ist durch die Bilder der Basisvektoren hinreichend definiert.
2. Jede Abbildung $B \longrightarrow W$ einer linear unabhängigen Menge B in einen Vektorraum W lässt sich zu einer linearen Abbildung $\langle B \rangle \longrightarrow W$ fortsetzen.

7.1 Lemma

Sei $\varphi : V \longrightarrow W$ eine lineare Abbildung und $\widetilde{V}$ bzw. $\widetilde{W}$ ein Unterraum von V bzw. W. Dann ist $\varphi(\widetilde{V}) = \{\varphi(v) \mid v \in V\}$ bzw. $\varphi^{-1}(\widetilde{W}) = \{v \in V \mid \varphi(v) \in W\}$ ein Unterraum von W bzw. V.

Beweis

Sei $w_1, w_2 \in \varphi(V)$. Dann gibt es $v_1, v_2 \in V$ mit $\varphi(v_1) = w_1$ und $\varphi(v_2) = w_2$. Es folgt $\lambda_1 \cdot w_1 + \lambda_2 \cdot w_2 = \lambda_1 \cdot \varphi(v_1) + \lambda_2 \cdot \varphi(v_2) = \varphi(\lambda_1 \cdot v_1 + \lambda_2 \cdot v_2)$. Wegen $\lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 \in V$ gilt damit $\lambda_1 \cdot w_1 + \lambda_2 \cdot w_2 \in \varphi(V)$.

Sei nun $v_1, v_2 \in \varphi^{-1}(W)$, d.h. es gilt $\varphi(v_1), \varphi(v_2) \in W$. Es folgt $\varphi(\lambda_1 \cdot v_1 + \lambda_2 \cdot v_2) = \lambda_1 \cdot \varphi(v_1) + \lambda_2 \cdot \varphi(v_2) \in W$, also $\lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 \in \varphi^{-1}(W)$.

7.2 Definition / Bemerkung

Sei $\varphi : V \longrightarrow W$ eine lineare Abbildung. Dann ist Bild $(\varphi) = \varphi(V)$ und Kern $(\varphi) = \varphi^{-1}(\{0\})$. Nach Lemma 7.1 ist Kern (φ) bzw. Bild (φ) ein Unterraum von V bzw. W.

7.3 Lemma

Sei $\varphi : V \longrightarrow W$ linear. Dann gilt: φ injektiv $\Longleftrightarrow$ Kern $\varphi = \{0\}$.

Beweis

Sei φ injektiv und $v \in$ Kern φ. Es folgt $\varphi(v) = 0 = \varphi(0)$ und daher $v = 0$. Also gilt Kern $\varphi = \{0\}$.

Sei nun Kern $\varphi = \{0\}$ und $\varphi(v) = \varphi(w)$. Dann gilt $0 = \varphi(v) - \varphi(w) = \varphi(v - w)$, also $v - w \in$ Kern φ. Damit ist $v - w = 0$, d.h $v = w$.

7.4 Lemma

Sei $\varphi : V \longrightarrow W$ linear und $M \subseteq V$ eine Teilmenge. Dann gilt $\varphi(\langle M \rangle) = \langle \varphi(M) \rangle$.

Beweis

Offenbar gilt $\varphi(M) \subseteq \varphi(\langle M \rangle)$. Nach Satz 4.7 ist $\langle \varphi(M) \rangle$ der kleinste Unterraum, der $\varphi(M)$ enthält. Da nach Lemma 7.1 $\varphi(\langle M \rangle)$ ein Unterraum ist, gilt also $\langle \varphi(M) \rangle \subseteq \varphi(\langle M \rangle)$.

Sei nun $v \in \varphi(\langle M \rangle)$, d.h. $v = \varphi(\sum \lambda_i m_i) = \lambda_i \sum \varphi(m_i)$ für $m_i \in M$. Wegen $\varphi(m_i) \in \varphi(M)$ folgt $v \in \langle \varphi(M) \rangle$, also $\varphi(\langle M \rangle) \subseteq \langle \varphi(M) \rangle$.

7.5 Satz (Dimensionssatz für lineare Abbildungen)

Sei $\varphi : V \longrightarrow W$ eine lineare Abbildung mit $\dim V < \infty$. Dann gilt $\dim V = \dim$ Bild $\varphi + \dim$ Kern φ.

Beweis

Sei $b_1, \ldots, b_r$ eine Basis von Kern φ. Nach Satz 4.16 können wir $b_1, \ldots, b_r$ zu einer Basis $b_1, \ldots, b_r, c_1, \ldots, c_s$ von V ergänzen. Sei dann $U = \langle c_1, \ldots, c_s \rangle$. Wegen $v \in V \Longleftrightarrow v = \sum \lambda_i b_i + \sum \mu_i c_i = u + w$ für $u \in \operatorname{Kern} \varphi$ und $w \in U \Longleftrightarrow v \in U \ + \ \operatorname{Kern} \varphi$ gilt dann $V = U \ + \ \operatorname{Kern} \varphi$.

Mit Satz 4.20 folgt nun

$$\begin{aligned}\dim(\operatorname{Kern}\varphi \ \cap\ U) &= \dim\operatorname{Kern}\varphi + \dim U - \dim(\operatorname{Kern}\varphi \ +\ U)\\ &= \dim\operatorname{Kern}\varphi + \dim U - \dim V\\ &= r + s - (r+s)\\ &= 0\end{aligned}$$

und da für jeden Vektorraum $W \neq \{0\}$ stets $\dim W > 0$ gilt, erhält man $\operatorname{Kern}\varphi \ \cap\ U = \{0\}$.

Man betrachte dann die lineare Abbildung $\psi : u \in U \longmapsto \varphi(u) \in W$. Wegen $\psi(v) = 0 \Longleftrightarrow v \in \operatorname{Kern}\varphi \ \cap\ U \Longleftrightarrow v = 0$ gilt Kern $\psi = \{0\}$, d.h. ψ ist injektiv. Daher ist $\psi : U \longrightarrow \varphi(U)$ isomorph und es folgt $\dim\varphi(U) = \dim U = s$.

Schließlich gilt $v \in$ Bild $\varphi = \varphi(V) = \varphi(\text{Kern } \varphi\ +\ U) \Longleftrightarrow v = \varphi(u{+}w) = \varphi(u){+}\varphi(w) = \varphi(u)$ für $u \in U$ und $w \in$ Kern $\varphi \Longleftrightarrow v \in \varphi(U)$, also dim Bild $\varphi = \dim\varphi(U) = s$. Damit ist $\dim V = r + s =$ dim Kern $\varphi +$ dim Bild φ.

7.6 Korollar

Seien V und W Vektorräume mit $\dim V = \dim W < \infty$ und sei $\varphi : V \longrightarrow W$ linear. Dann ist äquivalent:

1. φ ist injektiv
2. φ ist surjektiv
3. φ ist bijektiv

Beweis

1$\Longrightarrow$2 Sei φ injektiv. Dann gilt nach Lemma 7.3 Kern $\varphi = \{0\}$ und mit Satz 7.5 folgt dim Bild $\varphi = \dim V -$ dim Kern $\varphi = \dim W - \dim\{0\} = \dim W$. Wegen Bild $\varphi \subseteq W$ gilt Bild $\varphi = W$, d.h. φ ist surjekiv.

2$\Longrightarrow$1 Sei φ surjektiv. Dann ist Bild $\varphi = \varphi(V) = W$ und es folgt dim Kern $\varphi = \dim V -$ dim Bild $\varphi = \dim W - \dim W = 0$. Also ist Kern $\varphi = \{0\}$, d.h. φ ist injektiv.

1$\Longleftrightarrow$3 Sei φ injektiv. Dann ist φ surjektiv und damit bijektiv. Falls φ bijektiv ist, ist φ nach Definition injektiv.

7.7 Definition

Seien V und W endlich-dimensionale K-Vektorräume und $\alpha : V \longrightarrow W$ linear. Weiter sei $A = \{a_1, \ldots, a_n\}$ bzw. $B = \{b_1, \ldots, b_m\}$ eine Basis von V bzw. W mit $\alpha(a_j) = \sum\limits_{i=1}^{m} c_{ij} b_i$. Dann ordnen wir die Koeffizienten $c_{1j}, \ldots, c_{mj} \in K$ der j-ten Spalte der Matrix $M_\alpha(A, B)$ zu.

$$M_\alpha(A,B) = \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{m1} & \cdots & c_{mn} \end{pmatrix} \in K^{m \times n}$$

wird als Darstellungsmatrix der linearen Abbildung α bzgl. der Basen A und B bezeichnet.

Beispiel

Seien

$$\alpha : \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \longmapsto \begin{pmatrix} 6x - 2y \\ x + y \end{pmatrix} \in \mathbb{R}^2$$

und die Basen

$$A = \{\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}\} \text{ und } B = \{\begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\}$$

von $\mathbb{R}^2$ gegeben. Wegen

$$\alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 6 \\ 1 \end{pmatrix} = 3 \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} - 2 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

und

$$\alpha \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ 2 \end{pmatrix} = 2 \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

ist

$$M_\alpha(A,B) = \begin{pmatrix} 3 & 2 \\ -2 & 0 \end{pmatrix}.$$

Bemerkung

Seien V und W endlich-dimensionale K-Vektorräume und $M_\alpha(A,B)$ die Darstellungsmatrix einer linearen Abbildung α bzgl. der Basen $A = \{a_1, \ldots, a_n\}$ bzw. $B = \{b_1, \ldots, b_m\}$ von V bzw. W. Seien weiter $\varphi : V \longrightarrow K^n$ und $\psi : W \longrightarrow K^m$ die Kooardinatenabbildungen von V und W bzgl. der Basen A und B. Dann gilt

$$M_\alpha(A,B) \cdot \varphi(v) = \psi\big(\alpha(v)\big)$$

für alle $v \in V$. Man erhält also das Schema

$$
\begin{tikzcd}
\{a_1,\dots,a_n\}\ V \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & W\ \{b_1,\dots,b_m\} \arrow[d, "\Psi"] \\
K^n \arrow[r, "M_\alpha(A,B)"'] & K^m
\end{tikzcd}
$$

Beweis

Sei $v \in V$ mit $v = \sum\limits_{j=1}^{n} \lambda_j a_j$ und sei $M_\alpha(A,B) = (c_{ij})$, d.h. $\alpha(a_j) = \sum\limits_{i=1}^{m} c_{ij} b_i$. Dann gilt

$$\varphi(v) = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$

und es folgt

$$M_\alpha(A,B) \cdot \varphi(v) = \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{m1} & \cdots & c_{mn} \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} \sum\limits_{j=1}^{n} c_{1j} \cdot \lambda_j \\ \vdots \\ \sum\limits_{j=1}^{n} c_{mj} \cdot \lambda_j \end{pmatrix}.$$

Andererseits gilt $\alpha(v) = \alpha(\sum\limits_{j=1}^{n} \lambda_j a_j) = \sum\limits_{j=1}^{n} \lambda_j \alpha(a_j) = \sum\limits_{j=1}^{n} \lambda_j (\sum\limits_{i=1}^{m} c_{ij} b_i) = \sum\limits_{i=1}^{m} (\sum\limits_{j=1}^{n} \lambda_j c_{ij}) b_i$, d.h.

$$\psi\big(\alpha(v)\big) = \begin{pmatrix} \sum\limits_{j=1}^{n} c_{1j} \cdot \lambda_j \\ \vdots \\ \sum\limits_{j=1}^{n} c_{mj} \cdot \lambda_j \end{pmatrix} = M_\alpha(A,B) \cdot \varphi(v).$$

Bemerkung

Sei A eine $(m \times n)$-Matrix. Dann ist $\alpha : v \in K^n \longmapsto Av \in K^m$ linear und wird bzgl. der Standardbasen von K^n und K^m durch A dargestellt.

Beweis

Mit Satz 6.4 folgt folgt unmittelbar die Linearität von α. Sei nun $A = (a_{ij})$ und $e_1, \dots, e_n$ bzw. $f_1, \dots, f_m$ die Standardbasis von K^n bzw. K^m. Dann folgt die Behauptung aus $\alpha(e_j) = \sum\limits_{i=1}^{m} a_{ij} f_i$.

7.8 Satz

Seien $A = \{v_1, \dots, v_n\}$, $B = \{w_1, \dots, w_m\}$ und $C = \{z_1, \dots, z_p\}$ Basen der K-Vektorräume V, W und Z. Seien weiter lineare Abbildungen $\alpha : V \longrightarrow W$ und $\beta : W \longrightarrow Z$ mit den Darstellungsmatrizen $M_\alpha(A, B)$ und $M_\beta(B, C)$ gegeben. Dann ist

$$M_{\beta\circ\alpha}(A, C) = M_\beta(B, C) \cdot M_\alpha(A, B)$$

die Darstellungsmatrix von $\beta \circ \alpha$.

Beweis

Sei $M_\alpha(A, B) = (a_{ij})$ und $M_\beta(B, C) = (b_{ki})$ sowie $M_{\beta\circ\alpha}(A, C) = (c_{kj})$ für $1 \leq i \leq m$, $1 \leq j \leq n$ und $1 \leq k \leq p$. Damit gilt $\alpha(v_j) = \sum\limits_{i=1}^{m} a_{ij} w_i$, $\beta(w_i) = \sum\limits_{k=1}^{p} b_{ki} z_k$ und $\beta \circ \alpha(v_j) = \sum\limits_{k=1}^{p} c_{kj} z_k$. Weiter folgt

$$\beta \circ \alpha(v_j) = \beta\big(\alpha(v_j)\big) = \beta(\sum_{i=1}^{m} a_{ij} w_i) = \sum_{i=1}^{m} a_{ij} \beta(w_i) = \sum_{i=1}^{m} a_{ij} (\sum_{k=1}^{p} b_{ki} z_k) = \sum_{k=1}^{p} (\sum_{i=1}^{m} a_{ij} b_{ki}) z_k.$$

Aus der Eindeutigkeit der Basisdarstellung erhält man somit $c_{kj} = \sum\limits_{i=1}^{m} b_{ki} a_{ij}$ für alle $1 \leq k \leq p$ und $1 \leq j \leq n$. Also gilt $M_{\beta\circ\alpha}(A, C) = M_\beta(B, C) \cdot M_\alpha(A, B)$.

7.9 Satz

Für einen endlich-dimensionalen Vektorraum V ist die lineare Abbildung $\alpha : V \longrightarrow W$ genau dann ein Isomorphismus, wenn eine (und damit jede) darstellende Matrix von α invertierbar ist. Insbesondere gilt dann für Basen A und B von V und W stets

$$M_\alpha(A, B)^{-1} = M_{\alpha^{-1}}(B, A).$$

Beweis

1 Sei zunächst $\alpha : V \longrightarrow W$ ein Isomorphismus. Dann ist auch W endlich-dimensional mit $\dim V = \dim W$. Weiter existiert das Inverse $\alpha^{-1} : W \longrightarrow V$ mit $\alpha^{-1} \circ \alpha = \mathrm{id}$.

Die Identität id wird bzgl. einer festgewählten Basis A von V durch die Einheitsmatrix $M_{\mathrm{id}}(A, A) = 1_n$ dargestellt. Nach Satz 7.8 folgt damit $1_n = M_{\alpha^{-1}\circ\alpha}(A, A) = M_{\alpha^{-1}}(B, A) \cdot M_\alpha(A, B)$. Also ist $M_\alpha(A, B)$ invertierbar mit $M_\alpha(A, B)^{-1} = M_{\alpha^{-1}}(B, A)$.

2 Sei nun die Darstellungsmatrix $M = M_\alpha(A, B)$ der linearen Abbildung α invertierbar. Insbesondere ist dann M quadratisch, d.h. es gilt $\dim V = \dim W$.

Für die Koordinatenabbildung $\psi : W \longrightarrow K^n$ gilt $\alpha(v) = 0 \Longleftrightarrow \psi\big(\alpha(v)\big) = 0$. Mit der Koordinatenabbildung $\varphi : V \longrightarrow K^n$ folgt dann wegen $\psi\big(\alpha(v)\big) = M \cdot \varphi(v)$ auch $\alpha(v) = 0 \Longleftrightarrow M \cdot \varphi(v) = 0$.

Damit gilt für $v \in \text{Kern}\ \alpha$ stets $\varphi(v) = 1_n \cdot \varphi(v) = M^{-1}M \cdot \varphi(v) = M^{-1} \cdot 0 = 0 \Longleftrightarrow v = 0$, d.h. $\text{Kern}\ \alpha = \{0\}$. Daher ist α injektiv und nach Korollar 7.6 bijektiv.

7.10 Definition / Bemerkung

Seien A und B zwei Basen eines Vektorraumes V. Dann wird die Basistransformation $A \longrightarrow B$ durch die Matrix $P = M_{\text{id}}(A, B)$ beschrieben. Nach Satz 7.9 ist P invertierbar und wegen $\text{id}^{-1} = \text{id}$ gilt $P^{-1} = M_{\text{id}}(B, A)$. Andererseits beschreibt jede invertierbare Matrix einen Isomorphismus $V \longrightarrow V$, der sich als Basistransformation interpretieren lässt.

7.11 Satz

Seien V und W endlich-dimensionale Vektorräume und seien A und $\widetilde{A}$ bzw. B und $\widetilde{B}$ Basen von V bzw. W. Die Basistranformation $A \longrightarrow \widetilde{A}$ bzw. $B \longrightarrow \widetilde{B}$ sei durch eine Matrix P bzw. Q beschrieben. Dann gilt

$$M_\alpha(A, B) = Q^{-1} M_\alpha(\widetilde{A}, \widetilde{B}) P$$

für eine lineare Abbildung $\alpha : V \longrightarrow W$.

Beweis

Für Basistranformationen gilt $P = M_{\text{id}}(A, \widetilde{A})$ und $Q = M_{\text{id}}(B, \widetilde{B})$. Mit $\alpha = \alpha \circ \text{id}$ und Satz 7.8 folgt dann

$$M_\alpha(A, B) = M_{\alpha \circ \text{id}}(A, B) = M_\alpha(\widetilde{A}, B) \cdot M_{\text{id}}(A, \widetilde{A}) = M_\alpha(\widetilde{A}, B) \cdot P.$$

Mit $\alpha = \text{id} \circ \alpha$ ergibt sich weiter

$$M_\alpha(\widetilde{A}, B) = M_{\text{id} \circ \alpha}(\widetilde{A}, B) = M_{\text{id}}(\widetilde{B}, B) \cdot M_\alpha(\widetilde{A}, \widetilde{B}) = Q^{-1} M_\alpha(\widetilde{A}, \widetilde{B}).$$

Zusammen folgt die Behauptung.

7.12 Korollar

Seien A und B Basen des endlich-dimensionalen Vektorraums V und sei $\alpha : V \longrightarrow V$ linear. Die Basistranfsormation $A \longrightarrow B$ sei durch die Matrix T beschrieben. Dann gilt $M_\alpha(A, A) = T^{-1} M_\alpha(B, B) T$.

7.13 Lemma

Sei $A \in K^{m \times n}$ die Darstellungsmatrix der linearen Abbildung $\alpha : V \longrightarrow W$. Dann gilt rang $A = \dim$ Bild α.

Beweis

Sei α bzgl. der Basen $v_1, \ldots, v_n$ bzw. $w_1, \ldots, w_m$ von V bzw. W durch A dargestellt. Seien weiter $\varphi : V \longrightarrow K^n$ bzw. $\psi : W \longrightarrow K^m$ die Koordinatenabbildungen bzgl. dieser Basen. Dann liefert $\varphi(v_i)$ für $1 \leq i \leq n$ die Standardbasis $e_1, \ldots, e_n$ von K^n und es gilt $\psi\big(\alpha(v)\big) = A \cdot \varphi(v)$.

Daher ist $\psi\big(\alpha(v_i)\big) = A \cdot e_i = a_i$ die i-te Spalte der Matrix A. Mit Lemma 7.4 erhält man $\psi \circ \alpha(V) = \psi \circ \alpha(\langle v_1, \ldots, v_n \rangle) = \langle \psi \circ \alpha(v_1), \ldots, \psi \circ \alpha(v_n) \rangle = \langle a_1, \ldots, a_n \rangle$. Da rang A die Dimension des von den Spalten erzeugten Vektorraums ist, folgt $\dim \psi \circ \alpha(V) =$ rang A. Da zuletzt ψ ein Isomorphismus ist, folgt $\dim \psi\big(\alpha(V)\big) = \dim \alpha(V) = \dim$ Bild α.

7.14 Satz

Seien V und W endlich-dimensionale Vektorräume und $\alpha : V \longrightarrow W$ linear. Dann gibt es Basen B von V und C von W, so dass

$$M_\alpha(B, C) = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \\ \end{pmatrix} = \begin{pmatrix} 1_r & \\ & \end{pmatrix}$$

mit $r = \dim$ Bild α gilt.

Beweis

Seien $v_1, \ldots, v_r$ so gewählt, dass $\alpha(v_1), \ldots, \alpha(v_r)$ eine Basis von Bild α bilden. Man ergänze diese Basis zu einer Basis $C = \{\alpha(v_1), \ldots, \alpha(v_r), w_1, \ldots, w_t$ von W.

Sei nun $u_1, \ldots, u_s$ eine Basis von Kern α. Dann folgt $\dim V = \dim$ Bild α $+$ $\dim$ Kern $\alpha = r + s$. Man betrachte weiter die Linearkombination

$$\sum_{i=1}^{r} \lambda_i v_i + \sum_{i=1}^{s} \mu_i u_i = 0.$$

Es folgt

$$\begin{aligned} 0 &= \alpha(0) \\ &= \alpha(\sum_{i=1}^{r} \lambda_i v_i + \sum_{i=1}^{s} \mu_i u_i) \\ &= \sum_{i=1}^{r} \lambda_i \alpha(v_i) + \sum_{i=1}^{s} \mu_i \alpha(u_i) \\ &= \sum_{i=1}^{r} \lambda_i \alpha(v_i). \end{aligned}$$

Da die $\alpha(v_i)$ linear unabhängig sind, folgt damit $\lambda_i = 0$ für $1 \leq i \leq r$. Es bleibt

$$\sum_{i=1}^{s} \mu_i u_i = 0.$$

Da die u_i ebenfalls linear unabhängig sind, folgt $\mu_i = 0$ für $1 \leq i \leq s$. Also $v_1, \ldots, v_r, u_1, \ldots, u_s$ linear unabhängig und bilden insgesamt eine Basis B von V.

$M_\alpha(B, C)$ hat dann wegen $\alpha(v_i) = 0 \cdot \alpha(v_1) + \ldots + 1 \cdot \alpha(v_i) + \ldots + 0 \cdot w_t$ und $\alpha(u_i) = 0$ die gesuchte Form.

7.15 Korollar

Sei A eine $(m \times n)$-Matrix mit rang $A = r$. Dann gibt es invertierbare Matrizen $S \in K^{m \times m}$ und $T \in K^{n \times n}$ mit

$$S^{-1}AT = \begin{pmatrix} 1_r & \\ & \end{pmatrix}.$$

Beweis

Sei A die Darstellungsmatrix einer linearen Abbildung $\alpha : V \longrightarrow W$ bzgl. der Basis B_1 bzw. C_1 von V bzw. W. Nach Satz 7.14 gibt es dann eine Basis B_2 bzw. C_2 von V bzw. W mit

$$M_\alpha(B_2, C_2) = \begin{pmatrix} 1_r & \\ & \end{pmatrix}.$$

Beschreibe nun S bzw T die Basistransformation $B_2 \longrightarrow B_1$ bzw. $C_2 \longrightarrow C_1$. Dann sind S und T invertierbar und es gilt $S^{-1}AT = M_\alpha(B_2, C_2)$.

7.16 Satz

Seien $A \in M_{m \times n}(K)$ und $B \in M_{n \times p}(K)$ gegeben. Weiter seien $P \in M_{n \times n}(K)$ und $Q \in M_{m \times m}(K)$ invertierbar. Dann gilt

1. rang $A =$ rang A^t

2. rang $A \leq \min\{m, n\}$

3. rang $AB \leq \min\{$rang A, rang $B\}$

4. rang $A =$ rang QAP

Beweis

1 Es sind Zeilen- und Spaltenrang einer Matrix identisch. Weiter stimmt der Spaltenrang von A mit dem Zeilenrang von A^t überein. Daher folgt rang $A =$ rang A^t.

2 Da der Spaltenrang einer Matrix kleiner als die Anzahl der Spalten ist, gilt rang $A \leq n$. Da der Zeilenrang einer Matrix kleiner als die Anzahl der Zeilen ist, gilt rang $A \leq m$. Zusammen folgt die Behauptung.

3 Man betrachte $\alpha : v \in K^n \longrightarrow Av \in K^m$ und $\beta : v \in K^p \longrightarrow Bv \in K^n$. Dann wird α durch A beschrieben und es gilt nach Lemma 7.13 rang $A = \dim \alpha(K^n)$. Analog wird β durch B mit rang $B = \dim \beta(K^p)$ dargestellt.

Nach Satz 7.8 wird $\alpha \circ \beta$ – bzgl. der Standardbasen – durch AB dargestellt und es gilt rang $AB = \dim \alpha\big(\beta(K^p)\big)$. Es folgt einerseits $\beta(K^p) \subseteq K^n \Longrightarrow \alpha\big(\beta(K^p)\big) \subseteq \alpha(K^n) \Longrightarrow \dim \alpha\big(\beta(K^p)\big) \leq \dim \alpha(K^n)$.

Andererseits gilt $\dim V = \dim$ Bild $\varphi + \dim$ Kern φ für eine lineare Abbildung $\varphi : V \longrightarrow W$ mit $\dim V < \infty$. Wegen dim Kern $\varphi \geq 0$ folgt $\dim \varphi(V) = \dim$ Bild $\varphi \leq \dim V$. Speziell für $\alpha \circ \beta$ gilt also $\dim \alpha\big(\beta(K^p)\big) \leq \dim \beta(K^p)$.

Insgesamt folgt rang $AB = \dim \alpha\big(\beta(K^p)\big) \leq \min\{\dim \alpha(K^n), \dim \beta(K^p)\} = \min\{$rang A, rang $B\}$.

4 Nach 3 gilt rang $A \geq$ rang $AP \geq$ rang $APP^{-1} =$ rang A, also rang $A =$ rang AP. Analog erhält man rang $AP =$ rang QAP.

7.17 Satz

Sei $A \in M_{n \times n}(K)$. Dann ist A genau dann invertierbar, wenn rang $A = n$ gilt.

Beweis

Sei zunächst rang $A = n$. Nach Korollar 7.15 existieren dann invertierbare Matrizen $S, T \in M_{n\times n}(K)$ mit

$$S^{-1}AT = \begin{pmatrix} 1_n & \\ & \end{pmatrix}.$$

Wegen $S^{-1}AT \in M_{n\times n}(K)$ gilt sogar $S^{-1}AT = 1_n$. Für $B = TS^{-1}$ folgt dann $BA = TS^{-1}A = TS^{-1}ATT^{-1} = TT^{-1} = 1_n$, d.h. A ist invertierbar.

Sei nun A invertierbar. Dann ist nach Satz 7.9 die lineare Abbildung $\alpha : v \in K^n \longmapsto Av \in K^n$ ein Isomorphismus. Mit Lemma 7.13 folgt rang $A = \dim \text{Bild } \alpha = \dim K^n = n$.

Bemerkung

Nach Satz 7.17 ist eine quadratische Matrix genau dann invertierbar, wenn ihre Spalten linear unabhängig sind.

7.18 Definition

Zwei Matrizen $A, B \in K^{m\times n}$ heißen äquivalent, wenn es invertierbare Matrizen P, Q mit $B = QAP$ gibt. Zwei quadratische Matrizen $A, B \in K^{n\times n}$ heißen ähnlich, wenn es eine invertierbare Matrix T mit $B = T^{-1}AT$ gibt.

7.19 Satz

Es gilt A, B äquivalent $\Longleftrightarrow$ rang A = rang B. Daher ist Äquivalenz eine Äquivalenzrelation. Jede Äquivalenzklasse besitzt dabei ein Element der Form

$$\begin{pmatrix} 1_r & \\ & \end{pmatrix}.$$

Beweis

Seien A und B äquivalent. Dann gibt es eine invertierbare Matrizen S und T mit $B = SAT$. Mit Satz 7.16 folgt rang B = rang SAT = rang A.

Sei nun rang A = rang $B = r$. Dann gibt es nach Korollar 7.15 invertierbare Matrizen Q, R, S und T mit

$$Q^{-1}AR = \begin{pmatrix} 1_r & \\ & \end{pmatrix} = S^{-1}BT.$$

Es folgt $B = (SQ^{-1})A(RT^{-1})$, d.h. A und B sind ähnlich.

Da zwei Matrizen A und B genau dann äquivalent sind, wenn rang A = rang B gilt, sind Reflexivität, Symmetrie und Transitivität offensichtlich.

Zuletzt gilt für eine Matrix A wegen Korollar 7.15 stets

$$\begin{pmatrix} 1_r & \\ & \end{pmatrix} \in [A].$$

8 Lineare Gleichungssysteme

8.1 Definition

Für $1 \leq i \leq m$ und $1 \leq j \leq n$ sei $a_{ij} \in K$ und $b_i \in K$. Ein System

$$\begin{array}{ccccccccccc} a_{11} & x_1 & + & a_{12} & x_2 & + & \cdots & + & a_{1n} & x_n & = & b_1 \\ a_{21} & x_1 & + & a_{22} & x_2 & + & \cdots & + & a_{2n} & x_n & = & b_2 \\ & & \vdots & & & & & & & & \vdots & \\ a_{m1} & x_1 & + & a_{m2} & x_2 & + & \cdots & + & a_{mn} & x_n & = & b_m \end{array}$$

von Gleichungen in den Unbekannten $x_1, \ldots, x_n$ heißt lineares Gleichungssystem. Das System heißt homogen, falls $b_i = 0$ für alle $1 \leq i \leq m$ gilt. Anderenfalls heißt es inhomogen.

Sei

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1_n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \in M_{m \times n}(K),\ b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in K^m \text{ und } x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Dann wird das Gleichungssystem durch $Ax = b$ beschrieben.

Unter $(A \mid b)$ verstehen wir die Matrix

$$\begin{pmatrix} a_{11} & \cdots & a_{1_n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{pmatrix} \in M_{m \times (n+1)}(K).$$

8.2 Satz

Ein lineares Gleichungssystem $Ax = b$ ist genau dann lösbar, wenn rang A = rang $(A \mid b)$ gilt. Insbesondere ist $Ax = b$ für rang $A = m$ mit $A \in K^{m \times n}$ stets lösbar.

Beweis

Sei a_j die j-te Spalte der Matrix A. Dann lässt sich das Gleichungssystem durch $\sum_{i=1}^{n} a_j x_j = b$ beschreiben. Es existiere nun eine Lösung $x \in K^n$, d.h. $x_j \in K$ für alle $1 \leq j \leq n$. In diesem Fall ist also b eine Linearkombination der Spalten a_j, d.h. $\dim \{a_1, \ldots, a_n\} = \dim \{a_1, \ldots, a_n, b\}$. Daher gilt rang $A =$ rang $(A \mid b)$.

Es sei nun rang $A =$ rang $(A \mid b)$. Wegen $\{a_1, \ldots, a_n\} \subseteq \{a_1, \ldots, a_n, b\}$ gilt nach Satz 4.7 zunächst $\langle a_1, \ldots, a_n \rangle \subseteq \langle a_1, \ldots, a_n, b \rangle$. Mit rang $A =$ rang $(A \mid b)$ folgt $\dim \langle a_1, \ldots, a_n \rangle = \dim \langle a_1, \ldots, a_n, b \rangle$ und damit $\langle a_1, \ldots, a_n \rangle = \langle a_1, \ldots, a_n, b \rangle$. Daher gilt $b \in \langle a_1, \ldots, a_n \rangle$, d.h. $b = \sum_{i=1}^{n} a_j x_j$ mit $x_j \in K$ für $1 \leq j \leq n$. Dann ist

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n$$

ein Lösung von $Ax = b$.

Sei nun rang $A = m$ für $A \in K^{m \times n}$. Offenbar gilt rang $A \leq$ rang $(A \mid b)$ und nach Satz 7.16 ist rang $(A \mid b) \leq m$. Insgesamt folgt rang $A =$ rang $(A \mid b)$.

8.3 Satz

Sei $A \in M_{m \times n}(K)$. Dann ist die Lösungsmenge des homogenen linearen Gleichungssystems $Ax = 0$ ein Unterraum $L \subseteq K^n$ mit $\dim L = n -$rang A.

Beweis

Man betrachte die lineare Abbildung $\alpha : x \in K^n \longmapsto Ax$. Dann ist $L =$ Kern α ein Unterraum von K^n. Nach Lemma 7.13 gilt dim Bild $\alpha =$ rang A, d.h. $n = \dim K^n =$ dim Bild $\alpha +$ dim Kern $\alpha =$ rang $A + \dim L$.

Bemerkung

Für $A \in M_{m \times n}(K)$ mit $m < n$ betrachte man das System $Ax = 0$. Dann ist die Anzahl der Gleichungen kleiner als die Anzahl der Unbekannten. Es folgt rang $A \leq m < n$ und daher $\dim L = n -$rang $A > 0$. In diesem Fall gibt es also außer $x = 0$ noch weitere Lösungen.

8.4 Satz

Sei $A \in M_{m\times n}(K)$ und $b \in K^m$. Weiter sei $L = \{x \in K^n \mid Ax = 0\}$ der Lösungsraum von $Ax = 0$. Hat dann das System $Ax = b$ eine Lösung $x_0 \in K^n$, so ist $x_0 + L = \{x_0 + v \mid v \in L\}$ die Lösungsmenge von $Ax = b$.

Beweis

Sei $v \in L$. Dann gilt $A(x_0+v) = Ax_0+Av = b+0 = b$, d.h. x_0+v ist eine Lösung von $Ax = b$. Sei nun $x_1 \in K^n$ eine beliebige Lösung. Dann folgt $A(x_1 - x_0) = Ax_1 - Ax_0 = b - b = 0$, d.h. $x_1 - x_0 \in L$. Schließlich gilt $x_1 = x_0 + (x_1 - x_0) \in x_0 + L$.

Bemerkung

1. Die Lösungsmenge von $Ax = b$ ist allgemein kein Unterraum von K^n.
2. Auch für $A \in M_{m\times n}(K)$ mit $m < n$ kann das System $Ax = b$ keine Lösung haben.

8.5 Satz

Sei $A \in M_{n\times n}(K)$ eine quadratische Matrix. Dann sind äquivalent:

1. $Ax = 0$ hat nur die Lösung $x = 0$
2. $Ax = b$ ist für alle $b \in K^n$ lösbar
3. rang $A = n$
4. A ist invertierbar

Beweis

1 $\Longleftrightarrow$ 3 Nach Satz 8.3 gilt $\dim L = n-$rang A für den Lösungsraum L von $Ax = 0$. Das System hat offenbar genau dann nur die Lösung $x = 0$, wenn $\dim L = 0$ gilt. Es folgt rang $A = n$.

3 $\Longleftrightarrow$ 4 Nach Satz 7.17 gilt rang $A = n \Longleftrightarrow A$ ist invertierbar.

4 $\Longrightarrow$ 2 Da A invertierbar ist, existiert eine Matrix $B \in M_{n\times n}(K)$ mit $AB = 1_n$. Für $x = Bb$ gilt dann $Ax = ABb = 1_n b = b$.

2 $\Longrightarrow$ 1 Da für alle $b \in K^n$ ein $x \in K^n$ mit $Ax = b$ existiert, ist die lineare Abbildung $\alpha : x \in K^n \longmapsto Ax \in K^n$ surjektiv. Es folgt $\dim K^n = \dim \text{Bild } \alpha + \dim \text{Kern } \alpha = \dim K^n + \dim \text{Kern } \alpha \Longrightarrow \dim \text{Kern } \alpha = 0$. Kern α ist aber der Lösungsraum von $Ax = 0$.

Bemerkung

Zur praktischen Lösung des linearen Gleichungssystems $Ax = b$ bringt man die Matrix $(A \mid b)$ mittels des Gauß-Algorithmus auf eine Zeilenstufenform $(\widetilde{A} \mid \widetilde{b})$. Elementare Zeilenoperationen beeinflussen dabei die Lösungsmenge nicht. Dem System $\widetilde{A}x = \widetilde{b}$ liest man dann durch schrittweises Auflösen und Einsetzen die Lösungsmenge ab.

9 Determinanten

Bemerkung

Wir betrachten eine Matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{R}).$$

Dann ist A genau dann invertierbar, wenn die Spaltenvektoren linear unabhängig sind. Dies ist genau dann der Fall, wenn nicht beide Vektoren

$$v = \begin{pmatrix} a \\ c \end{pmatrix} \text{ und } w = \begin{pmatrix} b \\ d \end{pmatrix}$$

auf einer Gerade liegen. Sei dann F der Flächeninhalt des von v und w aufgespannten Parallelogramms. Dann gilt $F = 0 \Longleftrightarrow v$ und w liegen auf einer Gerade. Wegen $F = |ad - bc|$ gilt $F = 0 \Longleftrightarrow ad - bc = 0$ und man erhält: A invertierbar $\Longleftrightarrow ad - bc \neq 0$.

9.1 Definition

Sei V ein K-Vektorraum und $V^n = V \times \ldots \times V = \{(v_1, \ldots, v_n) \mid v_i \in V \text{ für } 1 \leq i \leq n\}$ die Menge der n-Tupel für ein $0 < n \in \mathbb{N}$. Man betrachte dann eine Abbildung $\varphi : V^n \longrightarrow K$ mit

1. $\varphi(v_1, \ldots, v_{i-1}, v_i + \widetilde{v}_i, v_{i+1}, \ldots, v_n) = \varphi(v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_n) + \varphi(v_1, \ldots, v_{i-1}, \widetilde{v}_i, v_{i+1}, \ldots, v_n)$

2. $\varphi(v_1, \ldots, v_{i-1}, \lambda \cdot v_i, v_{i+1}, \ldots, v_n) = \lambda \cdot \varphi(v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_n)$.

Dann ist φ in jeder Komponente linear und wird als Multilinearform (oder n-Linearform) bezeichnet. Für $n = 2$ heißt φ bilinear.

Bemerkung

Durch komponentenweise definierte Verknüpfungen wird V^n zu einem K-Vektorraum. Eine Multilinearform $V^n \longrightarrow K$ ist aber i.A. keine lineare Abbildung. Etwa gilt $\varphi(v+\widetilde{v}, w) = \varphi(v,w) + \varphi(\widetilde{v}, w) \neq \varphi(v,w) + \varphi(\widetilde{v}, 0)$ für $n=2$.

9.2 Definition

Eine Multilinearform $\varphi : V^n \longrightarrow K$ heißt alternierend, wenn $\varphi(v_1, \ldots, v_n) = 0$ für alle linear abhängigen Tupel $(v_1, \ldots, v_n) \in V^n$ gilt. Die Abbildung φ heißt ausgeartet, wenn für alle $v_1, \ldots, v_n \in V$ stets $\varphi(v_1, \ldots, v_n) = 0$ gilt.

Beispiel

Es sei $V = K^2$. Dann betrachte man die Abbildung $\varphi : V^2 \longrightarrow K$ definiert durch

$$\varphi(\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix}) = ad - bc.$$

Wegen

$$\begin{aligned}
\varphi(\begin{pmatrix} a \\ c \end{pmatrix} + \begin{pmatrix} \widetilde{a} \\ \widetilde{c} \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix}) &= \varphi(\begin{pmatrix} a+\widetilde{a} \\ c+\widetilde{c} \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix}) \\
&= (a+\widetilde{a})d - b(c+\widetilde{c}) \\
&= ad - bc + \widetilde{a}d - b\widetilde{c} \\
&= \varphi(\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix}) + \varphi(\begin{pmatrix} \widetilde{a} \\ \widetilde{c} \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix})
\end{aligned}$$

und

$$\begin{aligned}
\varphi(\lambda \cdot \begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix}) &= \varphi(\begin{pmatrix} \lambda \cdot a \\ \lambda \cdot c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix}) \\
&= (\lambda \cdot a)d - b(\lambda \cdot c) \\
&= \lambda \cdot (ad - bc) \\
&= \lambda \cdot \varphi(\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix})
\end{aligned}$$

ist φ linear in der ersten Komponenten. Analog folgt die Linearität in der zweiten Komponente, d.h. φ ist bilinear. Sind nun

$$\begin{pmatrix} a \\ c \end{pmatrix} \text{ und } \begin{pmatrix} b \\ d \end{pmatrix}$$

linear abhängig, so gilt

$$\begin{pmatrix} b \\ d \end{pmatrix} = \lambda \cdot \begin{pmatrix} a \\ c \end{pmatrix}.$$

Es folgt

$$\varphi(\begin{pmatrix} a \\ c \end{pmatrix}, \lambda \cdot \begin{pmatrix} a \\ c \end{pmatrix}) = \lambda \cdot \varphi(\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} a \\ c \end{pmatrix}) = \lambda \cdot (ac - ac) = 0,$$

d.h. φ ist alternierend. Zuletzt gilt $0 \in K$ und $1 \in K$ mit

$$\varphi(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}) = 1,$$

also ist φ nicht ausgeartet.

9.3 Lemma

Sei $\varphi : V^n \longrightarrow K$ eine Multilinearform. Dann ist äquivalent:

1. φ ist alternierend
2. $\varphi(v_1, \ldots, v_n) = 0$ falls es $1 \leq i, j \leq n$ mit $i \neq j$ und $v_i = v_j$ gibt

Beweis

1$\Longrightarrow$2 Sei φ alternierend und $v_i = v_j$ für $1 \leq i < j \leq n$. Dann sind $v_1, \ldots, v_n$ linear abhängig, d.h. es gilt $\varphi(v_1, \ldots, v_n) = 0$.

2$\Longrightarrow$1 Seien $v_1, \ldots, v_n$ linear abhängig. Dann existiert ein $\lambda_j \neq 0$ mit $1 \leq j \leq n$ und $\sum\limits_{i=1}^{n} \lambda_i v_i = 0$. Es folgt

$$v_j = \sum_{i \neq j} \frac{\lambda_i}{\lambda_j} v_i$$

und damit

$$\begin{aligned} \varphi(v_1, \ldots, v_n) &= \varphi(v_1, \ldots, v_{j-1}, \sum_{i \neq j} \tfrac{\lambda_i}{\lambda_j} v_i, v_{j+1}, \ldots, v_n) \\ &= \tfrac{\lambda_1}{\lambda_j} \cdot \varphi(v_1, \ldots, v_{j-1}, v_1, v_{j+1}, \ldots, v_n) \\ &+ \ldots \\ &+ \tfrac{\lambda_n}{\lambda_j} \cdot \varphi(v_1, \ldots, v_{j-1}, v_n, v_{j+1}, \ldots, v_n) \quad = \quad 0. \end{aligned}$$

9.4 Lemma

Sei $\varphi : V^n \longrightarrow K$ eine alternierende Multilinearform und $\pi \in S_n$ eine Permutation. Dann gilt für alle $v_i \in V$ mit $1 \leq i \leq n$ stets $\varphi(v_{\pi(1)}, \ldots, v_{\pi(n)}) = \operatorname{sign} \pi \cdot \varphi(v_1, \ldots, v_n)$.

Beweis

Zunächst betrachten wir eine Transposition $\tau \in S_n$ mit $\operatorname{sign} \tau = -1$. Sei dabei o.B.d.A. $\tau = (12)$, also $\tau(i) = i$ für $3 \leq i \leq n$. Mit Lemma 9.3 gilt nun

$$\begin{aligned} 0 &= \varphi(v_1 + v_2, v_1 + v_2, v_3, \ldots, v_n) \\ &= \varphi(v_1, v_2, v_3, \ldots, v_n) + \varphi(v_2, v_1, v_3, \ldots, v_n) \\ &= \varphi(v_1, \ldots, v_n) + \varphi(v_{\tau(1)}, \ldots, v_{\tau(n)}). \end{aligned}$$

Es folgt $\varphi(v_{\tau(1)}, \ldots, v_{\tau(n)}) = -\varphi(v_1, \ldots, v_n) = \operatorname{sign} \tau \cdot \varphi(v_1, \ldots, v_n)$.

Nach Satz 2.20 ist nun jede Permutation $\pi \in S_n$ ein Produkt von Transpositionen. Da sign ein Homomorphismus ist, folgt für $\pi = \tau_1 \cdots \tau_m$ sukzessive

$$\begin{aligned} \varphi(v_{\pi(1)}, \ldots, v_{\pi(n)}) &= \varphi(v_{\tau_1(\tau_2(\cdots(\tau_m(1))\cdots))}, \ldots, v_{\tau_1(\tau_2\cdots(\tau_m(n))\cdots))}) \\ &= \operatorname{sign} \tau_1 \cdot \varphi(v_{\tau_2(\cdots(\tau_m(1))\cdots)}, \ldots, v_{\tau_2\cdots(\tau_m(n))\cdots)}) \\ &= \cdots \\ &= \operatorname{sign} \tau_1 \cdots \operatorname{sign} \tau_m \cdot \varphi(v_1, \ldots, v_n) \\ &= \operatorname{sign} \tau_1 \cdots \tau_m \cdot \varphi(v_1, \ldots, v_n). \end{aligned}$$

Bemerkung

Im Folgenden betrachten wir Multilinearformen $V^n \longrightarrow K$ mit $\dim V = n$.

9.5 Lemma

Sei $v_1, \ldots, v_n$ eine Basis von V und $\varphi : V^n \longrightarrow K$ eine alternierende Multilinearform. Sei $u_i = \sum_{j=1}^{n} a_{ij} v_j$ für $a_{ij} \in K$ und $1 \leq i \leq n$. Dann gilt $\varphi(u_1, \ldots, u_n) = \varphi(v_1, \ldots, v_n) \cdot \sum_{\pi \in S_n} \operatorname{sign} \pi \cdot a_{1\pi(1)} \cdots a_{n\pi(n)}$.

Beweis

Es gilt

$$\begin{aligned}
\varphi(u_1,\dots,u_n) &= \varphi(\sum_{k_1=1}^{n} a_{1k_1}v_{k_1},\dots,\sum_{k_n=1}^{n} a_{nk_n}v_{k_n}) \\
&= \sum_{k_1=1}^{n} a_{1k_1}(\cdots(\sum_{k_n=1}^{n} a_{nk_n}\varphi(v_{k_1},\dots,v_{k_n}))\cdots) \\
&= \sum_{k_1=1}^{n}\cdots\sum_{k_n=1}^{n} a_{1k_1}\cdots a_{nk_n}\varphi(v_{k_1},\dots,v_{k_n}).
\end{aligned}$$

Nach Lemma 9.3 gilt $\varphi(v_{k_1},\dots,v_{k_n})=0$ für diejenigen Summanden mit $k_i=k_j$ für $1\le i,j\le n$ und $i\neq j$. Seien also $k_1,\dots,k_n$ paarweise verschieden, d.h. $\{k_1,\dots,k_n\}=\{1,\dots,n\}$. Dann existiert genau eine Permutation $\pi\in S_n$ mit $k_i=\pi(i)$ für $1\le i\le n$.

Mit Lemma 9.4 erhalten wir also insgesamt

$$\begin{aligned}
\varphi(u_1,\dots,u_n) &= \sum_{k_1=1}^{n}\cdots\sum_{k_n=1}^{n} a_{1k_1}\cdots a_{nk_n}\varphi(v_{k_1},\dots,v_{k_n}) \\
&= \sum_{\pi\in S_n} a_{1\pi(1)}\cdots a_{n\pi(n)}\varphi(v_{\pi(1)},\dots,v_{\pi(n)}) \\
&= \sum_{\pi\in S_n} a_{1\pi(1)}\cdots a_{n\pi(n)}\operatorname{sign}\pi\cdot\varphi(v_1,\dots,v_n) \\
&= \varphi(v_1,\dots,v_n)\cdot\sum_{\pi\in S_n}\operatorname{sign}\pi\cdot a_{1\pi(1)}\cdots a_{n\pi(n)}.
\end{aligned}$$

9.6 Lemma

Sei $\dim V=n$ und $\varphi: V^n\longrightarrow K$ eine nicht-ausgeartete, alternierende n-Linearform. Dann sind äquivalent:

1. $\varphi(v_1,\dots,v_n)=0$
2. $v_1,\dots,v_n$ linear abhängig

Beweis

2 $\Longrightarrow$ 1 Diese Implikation ist gerade die Definition einer alternierenden Multilinearform.

1 $\Longrightarrow$ 2 Sei $M=\{v_1,\dots,v_n\}$ linear unabhängig mit $\varphi(v_1,\dots,v_n)=0$. Wegen $\dim V=n$ bildet dann M eine Basis von V. Jeder Vektor $u_i\in V$ hat daher eine Darstellung $u_i=\sum_{j=1}^{n} a_{ij}v_j$ für $a_{ij}\in K$. Nach Lemma 9.5 folgt $\varphi(u_1,\dots,u_n)=\varphi(v_1,\dots,v_n)\cdot\sum_{\pi\in S_n}\operatorname{sign}\pi\cdot a_{1\pi(1)}\cdots a_{n\pi(n)}=0$. Damit ist φ aber ausgeartet.

9.7 Satz

Sei $v_1, \ldots, v_n$ eine Basis des K-Vektorraums V. Dann ist die Abbildung $\varphi : (u_1, \ldots, u_n) \in V^n \longmapsto \sum_{\pi \in S_n} \operatorname{sign} \pi \cdot a_{1\pi(1)} \cdots a_{n\pi(n)} \in K$ für $u_i = \sum_{j=1}^{n} a_{ij} v_j$ mit $a_{ij} \in K$ eine nicht ausgeartete, alternierende Multilinearform.

Beweis

Zunächst sieht man, dass φ wegen der Eindeutigkeit der Basisdarstellung wohldefiniert ist.

Sei nun $u_i = \sum_{j=1}^{n} a_{ij} v_j$ und $\widetilde{u}_i = \sum_{j=1}^{n} \widetilde{a}_{ij} v_j$. Dann gilt $u_i + \widetilde{u}_i = \sum_{j=1}^{n} (a_{ij} + \widetilde{a}_{ij}) v_j$ und damit

$$\begin{aligned}
\varphi(u_1, \ldots, u_i + \widetilde{u}_i, \ldots, u_n) &= \sum_{\pi \in S_n} \operatorname{sign} \pi \cdot a_{1\pi(1)} \cdots (a_{i\pi(i)} + \widetilde{a}_{i\pi(i)}) \cdots a_{n\pi(n)} \\
&= \sum_{\pi \in S_n} \operatorname{sign} \pi \cdot a_{1\pi(1)} \cdots a_{i\pi(i)} \cdots a_{n\pi(n)} \\
&+ \sum_{\pi \in S_n} \operatorname{sign} \pi \cdot a_{1\pi(1)} \cdots \widetilde{a}_{i\pi(i)} \cdots a_{n\pi(n)} \\
&= \varphi(u_1, \ldots, u_i, \ldots, u_n) + \varphi(u_1, \ldots, \widetilde{u}_i, \ldots, u_n).
\end{aligned}$$

Mit $\lambda \cdot u_i = \sum_{j=1}^{n} (\lambda \cdot a_{ij}) v_j$ folgt weiter

$$\begin{aligned}
\varphi(u_1, \ldots, \lambda \cdot u_i, \ldots, u_n) &= \sum_{\pi \in S_n} \operatorname{sign} \pi \cdot a_{1\pi(1)} \cdots (\lambda \cdot a_{i\pi(i)}) \cdots a_{n\pi(n)} \\
&= \lambda \cdot \sum_{\pi \in S_n} \operatorname{sign} \pi \cdot a_{1\pi(1)} \cdots a_{i\pi(i)} \cdots a_{n\pi(n)} \\
&= \lambda \cdot \varphi(u_1, \ldots, u_i, \ldots, u_n).
\end{aligned}$$

Insgesamt ist φ also multilinear.

Ferner betrachten wir das Tupel $(v_1, \ldots, v_n)$. Wegen $v_i = 0 \cdot v_1 + \ldots + 1 \cdot v_i + \ldots + 0 \cdot v_n$ gilt dann $a_{ii} = 1$ und $a_{ij} = 0$ für alle $1 \leq i, j \leq n$ mit $i \neq j$. Daher gilt $a_{1\pi(1)} \cdots a_{n\pi(n)} \neq 0$ nur für den Summand $\pi = 1 \in S_n$ mit $\operatorname{sign} \pi = 1$. Es folgt $\varphi(v_1, \ldots, v_n) = 1$, d.h. φ ist nicht ausgeartet.

Es bleibt zu zeigen, dass φ alternierend ist. Wir betrachten dazu die Transposition $(kl) = \tau \in S_n$, d.h. $\tau(i) = i$ für alle $i \notin \{k, l\}$. Wegen $A_n = \text{Kern sign}$ – also $A_n \cap A_n \tau = \emptyset$ – und

$|A_n\tau| = |A_n| = \frac{1}{2}|S_n|$ ist $S_n = A_n \dot\cup A_n\tau$ eine disjunkte Vereinigung. Es folgt

$$\begin{aligned}
\varphi(u_1,\ldots,u_n) &= \sum_{\pi\in A_n} \operatorname{sign}\pi \cdot a_{1\pi(1)}\cdots a_{k\pi(k)}\cdots a_{l\pi(l)}\cdots a_{n\pi(n)} \\
&+ \sum_{\pi\in A_n} \operatorname{sign}(\pi\cdot\tau) \cdot a_{1\pi(\tau(1))}\cdots a_{k\pi(\tau(k))}\cdots a_{l\pi(\tau(l))}\cdots a_{n\pi(\tau(n))} \\
&= \sum_{\pi\in A_n} \operatorname{sign}\pi \cdot a_{1\pi(1)}\cdots a_{k\pi(k)}\cdots a_{l\pi(l)}\cdots a_{n\pi(n)} \\
&+ \sum_{\pi\in A_n} \operatorname{sign}\pi \cdot \operatorname{sign}\tau \cdot a_{1\pi(1)}\cdots a_{k\pi(l)}\cdots a_{l\pi(k)}\cdots a_{n\pi(n)} \\
&= \sum_{\pi\in A_n} a_{1\pi(1)}\cdots a_{k\pi(k)}\cdots a_{l\pi(l)}\cdots a_{n\pi(n)} \\
&- \sum_{\pi\in A_n} a_{1\pi(1)}\cdots a_{k\pi(l)}\cdots a_{l\pi(k)}\cdots a_{n\pi(n)} \\
&= \sum_{\pi\in A_n} a_{1\pi(1)}\cdots a_{n\pi(n)} \cdot \big(a_{k\pi(k)}\cdot a_{l\pi(l)} - a_{k\pi(l)}\cdot a_{l\pi(k)}\big)
\end{aligned}$$

Sei nun $\sum\limits_{j=1}^{n} a_{kj}v_j = u_k = u_l = \sum\limits_{j=1}^{n} a_{lj}v_j$. Mit der Eindeutigkeit der Basisdarstellung folgt $a_{kj} = a_{lj}$ für alle $1 \le j \le n$, also insbesondere $a_{kk} = a_{lk}$ sowie $a_{kl} = a_{ll}$. Daher gilt $a_{k\pi(k)} \cdot a_{l\pi(l)} - a_{k\pi(l)} \cdot a_{l\pi(k)} = 0$, d.h. $\varphi(u_1,\ldots,u_l,\ldots,u_k,\ldots,u_n) = 0$. Damit ist φ nach Lemma 9.3 alternierend.

9.8 Satz

Sei $\dim V = n$ und seien ψ sowie φ nicht ausgeartete, alternierende n-Linearformen auf V. Dann gibt es genau ein $0 \neq \lambda \in K$ mit $\varphi(u_1,\ldots,u_n) = \lambda\cdot\psi(u_1,\ldots,u_n)$ für alle $u_i \in V$ mit $1 \le i \le n$.

Beweis

Sei $v_1,\ldots,v_n$ eine Basis von V. Für jeden Vektor $u_i \in V$ gilt dann $u_i = \sum\limits_{j=1}^{n} a_{ij}v_j$ mit $a_{ij} \in K$. Setze $b = \sum\limits_{\pi\in S_n} \operatorname{sign}\pi\cdot a_{1\pi(1)}\cdots a_{n\pi(n)}$. Mit Lemma 9.5 folgt nun $\varphi(u_1,\ldots,u_n) = b\cdot\varphi(v_1,\ldots,v_n)$ und $\psi(u_1,\ldots,u_n) = b\cdot\psi(v_1,\ldots,v_n)$.

Nach Lemma 9.6 gilt weiter $\varphi(v_1,\ldots,v_n) \neq 0$ und $\psi(v_1,\ldots,v_n) \neq 0$. Für $\lambda = \frac{\varphi(v_1,\ldots,v_n)}{\psi(v_1,\ldots,v_n)}$ folgt dann $\varphi(u_1,\ldots,u_n) = b\cdot\varphi(v_1,\ldots,v_n) = \lambda\cdot b\cdot\psi(v_1,\ldots,v_n) = \lambda\cdot\psi(u_1,\ldots,u_n)$.

Es sei nun ein μ mit $\varphi = \mu\cdot\psi$ gegeben. Für ein beliebiges linear unabhängigs Tupel $u_1,\ldots,u_n$ gilt $\psi(u_1,\ldots,u_n) \neq 0$ und daher $\mu = \frac{\varphi(u_1,\ldots,u_n)}{\psi(u_1,\ldots,u_n)} = \frac{b\cdot\varphi(v_1,\ldots,v_n)}{b\cdot\psi(v_1,\ldots,v_n)} = \frac{\varphi(v_1,\ldots,v_n)}{\psi(v_1,\ldots,v_n)} = \lambda$.

9.9 Lemma

Sei $\dim V = n < \infty$ und $\alpha : V \longrightarrow V$ ein Endomorphismus. Dann ist äquivalent:

1. α invertierbar und $v_1, \ldots, v_n$ linear unabhängig
2. $\alpha(v_1), \ldots, \alpha(v_n)$ linear unabhängig

Beweis

1 $\Longrightarrow$ 2 Sei $\sum\limits_{i=1}^{n} \lambda_i \alpha(v_i) = 0$ eine Linearkombination. Es folgt

$$\alpha(\sum_{i=1}^{n} \lambda_i v_i) = \sum_{i=1}^{n} \lambda_i \alpha(v_i) = 0 = \alpha(0).$$

Da α bijektiv und damit injektiv ist, ergibt sich $\sum\limits_{i=1}^{n} \lambda_i v_i = 0$. Aus der linearen Unabhängigkeit von $v_1, \ldots, v_n$ folgt schließlich $\lambda_i = 0$ für $1 \leq i \leq n$.

2 $\Longrightarrow$ 1 Sei $\sum\limits_{i=1}^{n} \lambda_i v_i = 0$ eine Linearkombination. Dann gilt

$$0 = \alpha(0) = \alpha(\sum_{i=1}^{n} \lambda_i v_i) = \sum_{i=1}^{n} \lambda_i \alpha(v_i).$$

Da $\alpha(v_1), \ldots, \alpha(v_n)$ linear unabhängig ist, folgt $\lambda_i = 0$ für $1 \leq i \leq n$.

Weiter bildet $\alpha(v_1), \ldots, \alpha(v_n)$ wegen $\dim V = n$ eine Basis, d.h. für alle Vektoren $u \in V$ gilt

$$u = \sum_{i=1}^{n} \mu_i \alpha(v_i) = \alpha(\sum_{i=1}^{n} \mu_i v_i).$$

Damit ist α surjektiv und nach Korollar 7.6 sogar bijektiv.

9.10 Definition / Satz

Sei $v_1, \ldots, v_n$ ein Basis von V und sei $\varphi : V^n \longrightarrow K$ eine nicht ausgeartete, alternierende Multilinearform. Für einen Endomorphismus $\alpha \in \mathrm{End}(V)$ wird die Determinante durch

$$\det \alpha = \frac{\varphi\big(\alpha(v_1), \ldots, \alpha(v_n)\big)}{\varphi(v_1, \ldots, v_n)}$$

definiert. Dabei ist $\det \alpha$ wohldefiniert und hängt weder von der Wahl der Basis noch von der Wahl der Multilinearform ab.

Beweis

Nach Lemma 9.6 gilt für Basisvektoren $\varphi(v_1,\dots,v_n)\neq 0$, d.h $\det\alpha$ ist wohldefiniert. Für eine weitere nicht ausgeartete, alternierende Multilinearform $\psi : V^n \longrightarrow K$ existiert nach Satz 9.8 ein $0\neq\lambda\in K$ mit $\varphi=\lambda\cdot\psi$. Es folgt

$$\frac{\varphi\big(\alpha(v_1),\dots,\alpha(v_n)\big)}{\varphi(v_1,\dots,v_n)}=\frac{\lambda\cdot\psi\big(\alpha(v_1),\dots,\alpha(v_n)\big)}{\lambda\cdot\psi(v_1,\dots,v_n)}=\frac{\psi\big(\alpha(v_1),\dots,\alpha(v_n)\big)}{\psi(v_1,\dots,v_n)},$$

d.h. $\det\alpha$ ist unabhängig von der Wahl der Multilinearform.

Es bleibt die Unabhängigkeit von der Wahl der Basis zu zeigen. Sei zunächst α nicht invertierbar. Dann ist $\alpha(v_1),\dots,\alpha(v_n)$ nach Lemma 9.9 für jede Basis $v_1,\dots,v_n$ linear abhängig, d.h. es gilt stets $\varphi\big(\alpha(v_1),\dots,\alpha(v_n)\big)=0 \Longleftrightarrow \det\alpha=0$.

Sei nun α invertierbar. Dann betrachte man die Abbildung

$$\psi : (u_1,\dots,u_n)\in V^n \longmapsto \varphi\big(\alpha(u_1),\dots,\alpha(u_n)\big)\in K.$$

Aus $\alpha(u_i+\widetilde{u}_i)=\alpha(u_i)+\alpha(\widetilde{u}_i)$ sowie $\alpha(\lambda\cdot u_i)=\lambda\cdot\alpha(u_i)$ und da φ eine n-Linearform ist, folgt die Multilinearität von ψ. Da φ alternierend ist, ist mit Lemma 9.9 auch ψ alternierend. Nach Lemma 9.6 folgt für linear unabhängige Vektoren $v_1,\dots,v_n$ stets $\varphi(v_1,\dots,v_n)\neq 0$ und nach Lemma 9.9 erhält man damit $\psi(v_1,\dots,v_n)\neq 0$. Insgesamt ist also ψ eine nicht ausgeartete, alternierende Multilinearform.

Mit Satz 9.8 existiert ein $0\neq\lambda\in K$ mit $\varphi=\lambda\cdot\psi$. Dieses $\lambda\in K$ ist eindeutig und daher von einer Basis $v_1,\dots,v_n$ unabhängig. Es folgt also stets

$$\frac{\varphi\big(\alpha(v_1),\dots,\alpha(v_n)\big)}{\varphi(v_1,\dots,v_n)}=\lambda.$$

9.11 Korollar

Sei $\dim V<\infty$ und $\alpha,\beta\in\mathrm{End}(V)$. Dann gilt

1. $\det(\alpha\circ\beta)=\det\alpha\cdot\det\beta$
2. $\det\alpha\neq 0 \Longleftrightarrow \alpha$ invertierbar
3. α invertierbar $\Longrightarrow \det\alpha^{-1}=(\det\alpha)^{-1}$

Beweis

2 Sei $v_1,\dots,v_n$ ein Basis von V und sei $\varphi : V^n\longrightarrow K$ eine nicht ausgeartete, alternierende Multilinearform. Dann gilt

$$\det\alpha=\frac{\varphi\big(\alpha(v_1),\dots,\alpha(v_n)\big)}{\varphi(v_1,\dots,v_n)}.$$

Nach Lemma 9.6 und Lemma 9.9 folgt dann $\det \alpha \neq 0 \iff \alpha(v_1), \ldots, \alpha(v_n)$ linear unabhängig $\iff \alpha$ invertierbar.

1 Sei zunächst β nicht invertierbar, d.h. $\det \beta = 0$. Nach Korollar 7.6 ist dann β nicht surjektiv. Also ist auch $\alpha \circ \beta$ nicht surjektiv, d.h. nicht invertierbar. Es folgt $\det \alpha \cdot \det \beta = \det \alpha \cdot 0 = 0 = \det(\alpha \circ \beta)$.

Sei nun β invertierbar. Nach Lemma 9.9 ist dann $\beta(v_1), \ldots, \beta(v_n)$ linear unabhängig und bildet somit eine Basis von V. Daher ist

$$\det \alpha = \frac{\varphi\big(\alpha(\beta(v_1)), \ldots, \alpha(\beta(v_n))\big)}{\varphi(\beta(v_1), \ldots, \beta(v_n))}$$

und es folgt

$$\begin{aligned} \det(\alpha \circ \beta) &= \tfrac{\varphi\left(\alpha\circ\beta(v_1),\ldots,\alpha\circ\beta(v_n)\right)}{\varphi(v_1,\ldots,v_n)} \\ &= \tfrac{\varphi\left(\alpha(\beta(v_1)),\ldots,\alpha(\beta(v_n))\right)}{\varphi(\beta(v_1),\ldots,\beta(v_n))} \cdot \tfrac{\varphi\left(\beta(v_1),\ldots,\beta(v_n)\right)}{\varphi(v_1,\ldots,v_n)} \\ &= \det \alpha \cdot \det \beta. \end{aligned}$$

3 Es gilt $\det \alpha^{-1} \cdot \det \alpha = \det(\alpha^{-1} \circ \alpha) = \det 1$ mit

$$\det 1 = \frac{\varphi\big(1(v_1), \ldots, 1(v_n)\big)}{\varphi(v_1, \ldots, v_n)} = \frac{\varphi(v_1, \ldots, v_n)}{\varphi(v_1, \ldots, v_n)} = 1.$$

Daher folgt $\det \alpha^{-1} = (\det \alpha)^{-1}$.

Bemerkung

Für $\alpha, \beta \in \mathrm{End}(V)$ gilt i.A. $\det(\alpha + \beta) \neq \det \alpha + \det \beta$.

9.12 Definition

Sei für $0 < n \in \mathbb{N}$ eine quadratische Matrix $A = (a_{ij}) \in M_{n\times n}(K)$ gegeben. Dann ist $\det A = \sum\limits_{\pi \in S_n} \operatorname{sign} \pi \cdot a_{1\pi(1)} \cdots a_{n\pi(n)}$ die Determinante von A.

Beispiel

Sei $A \in M_{2\times 2}(K)$ definiert durch

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

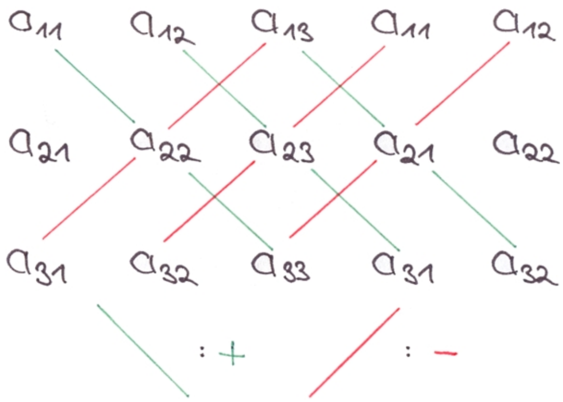
Wegen $S_2 = \{1, (12)\}$ gilt dann $\det A = \operatorname{sign} 1 \cdot a_{11} \cdot a_{22} + \operatorname{sign}(12) \cdot a_{12} \cdot a_{21} = a_{11} \cdot a_{22} - a_{12} \cdot a_{21}$.

Bemerkung

Sei $A \in M_{3\times 3}(K)$ definiert durch

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

Dann lässt sich $\det A$ durch die Regel von Sarrus



ausdrücken.

Beweis

Wegen $S_3 = \{1, (123), (321), (12), (13), (23)\}$ gilt $\det A = \operatorname{sign} 1 \cdot a_{11} \cdot a_{22} \cdot a_{33} + \operatorname{sign}(123) \cdot a_{12} \cdot a_{23} \cdot a_{31} + \operatorname{sign}(321) \cdot a_{13} \cdot a_{21} \cdot a_{32} + \operatorname{sign}(12) \cdot a_{12} \cdot a_{21} \cdot a_{33} + \operatorname{sign}(13) \cdot a_{13} \cdot a_{22} \cdot a_{31} + \operatorname{sign}(23) \cdot a_{11} \cdot a_{23} \cdot a_{32} = a_{11} \cdot a_{22} \cdot a_{33} + a_{12} \cdot a_{23} \cdot a_{31} + a_{13} \cdot a_{21} \cdot a_{32} - a_{12} \cdot a_{21} \cdot a_{33} - a_{13} \cdot a_{22} \cdot a_{31} - a_{11} \cdot a_{23} \cdot a_{32}$.

9.13 Satz

Sei $A \in M_{n\times n}(K)$. Dann gilt $\det A = \det A^t$.

Beweis

Sei $A = (a_{ij})$ und $A^t = B = (b_{ij})$, d.h. $b_{ij} = a_{ji}$. Dann gilt

$$\det A^t = \det B = \sum_{\pi \in S_n} \operatorname{sign} \pi \cdot b_{1\pi(1)} \cdots b_{n\pi(n)} = \sum_{\pi \in S_n} \operatorname{sign} \pi \cdot a_{\pi(1)1} \cdots a_{\pi(n)n}.$$

Da eine Permutation $\pi \in S_n$ bijektiv ist, existiert für alle $1 \leq i \leq n$ genau ein $1 \leq j \leq n$ mit $\pi(j) = i$, d.h. $a_{\pi(j)j} = a_{i\pi^{-1}(i)}$. Es folgt

$$\det A^t = \sum_{\pi \in S_n} \operatorname{sign} \pi \cdot a_{1\pi^{-1}(1)} \cdots a_{n\pi^{-1}(n)}.$$

Jedes Element des symmetrischen Gruppe $\pi \in S_n$ besitzt nun genau ein Inverses $\pi^{-1} \in S_n$, d.h. $\{\pi \mid \pi \in S_n\} = \{\pi^{-1} \mid \pi \in S_n\}$. Man erhält also

$$\det A^t = \sum_{\pi^{-1} \in S_n} \operatorname{sign} \pi \cdot a_{1\pi^{-1}(1)} \cdots a_{n\pi^{-1}(n)}.$$

Weiter gilt $1 = \operatorname{sign} 1 = \operatorname{sign} \pi\pi^{-1} = \operatorname{sign} \pi \cdot \operatorname{sign} \pi^{-1} \Longrightarrow \operatorname{sign} \pi = \operatorname{sign} \pi^{-1}$, d.h.

$$\det A^t = \sum_{\pi^{-1} \in S_n} \operatorname{sign} \pi^{-1} \cdot a_{1\pi^{-1}(1)} \cdots a_{n\pi^{-1}(n)} = \det A.$$

9.14 Satz

Sei $A \in M_{n \times n}(K)$ und $\alpha \in \mathrm{K^n}$ definiert durch $\alpha(v) = Av$. Dann gilt $\det \alpha = \det A$.

Beweis

Sei $\varphi : V \longrightarrow K$ eine nicht ausgeartete, alternierende Multilinearform mit $V = K^n$. Sei weiter $e_1, \ldots, e_n$ die Standardbasis von K^n, d.h.

$$\alpha(e_i) = Ae_i = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{pmatrix} = \sum_{j=1}^{n} b_{ij} e_j$$

mit $b_{ij} = a_{ji}$. Nach Lemma 9.5 gilt dann

$$\varphi\big(\alpha(e_1), \ldots, \alpha(e_n)\big) = \varphi(e_1, \ldots, e_n) \cdot \sum_{\pi \in S_n} \operatorname{sign} \pi \cdot b_{1\pi(1)} \cdots b_{n\pi(n)}.$$

Mit $A^t = (b_{ij})$ und Satz 9.13 erhält schließlich

$$\det \alpha = \frac{\varphi\big(\alpha(e_1), \ldots, \alpha(e_n)\big)}{\varphi(e_1, \ldots, e_n)} = \sum_{\pi \in S_n} \operatorname{sign} \pi \cdot b_{1\pi(1)} \cdots b_{n\pi(n)} = \det A^t = \det A.$$

9.15 Satz

Sei $A \in M_{n \times n}(K)$.

1. Die Matrix $\widetilde{A}$ erhalte man durch Anwendung einer Permutation $\pi \in S_n$ auf die Zeilen oder auf die Spalten von A. Dann gilt $\det \widetilde{A} = \operatorname{sign} \pi \cdot \det A$.

2. Durch Addition des Vielfachen einer Zeile bzw. einer Spalte von A zu einer anderen Zeile bzw. Spalte erhalte man die Matrix $\widetilde{A}$. Dann gilt $\det \widetilde{A} = \det A$.

3. Durch Multiplikation einer Zeile bzw. einer Spalte von A mit einem Skalar $\lambda \in K$ erhält man eine Matrix $\widetilde{A}$ mit $\det \widetilde{A} = \lambda \cdot \det A$. Insbesondere gilt $\det(\lambda \cdot A) = \lambda^n \cdot \det A$.

4. Es gilt $\det A = 0 \Longleftrightarrow \operatorname{rang} A < n$.

5. Für $1_n \in M_{n\times n}(K)$ gilt $\det 1_n = 1$.

6. Mit $B \in M_{n\times n}(K)$ folgt $\det AB = \det A \cdot \det B$.

7. Sei A invertierbar. Dann ist $\det A^{-1} = (\det A)^{-1}$.

8. Für ähnliche Matrizen A und B gilt $\det A = \det B$.

Beweis

Wegen $\det A = \det A^t$ sind die Aussagen entweder für die Zeilen oder die Spalten von A zu beweisen. Sei dann $\alpha : v \in K^n \longmapsto Av$ und $\varphi : V^n \longrightarrow K$ eine nicht ausgeartete, alternierende Multilinearform auf $V = K^n$. Weiter sei $e_1, \dots, e_n$ die Standardbasis von K, d.h. $\alpha(e_i) = Ae_i = a_i \in K^n$ liefert die i-te Spalte von A. Dann gilt

$$\det A = \det \alpha = \frac{\varphi\big(\alpha(e_1), \dots, \alpha(e_n)\big)}{\varphi(e_1, \dots, e_n)} = \frac{\varphi(a_1, \dots, a_n)}{\varphi(e_1, \dots, e_n)}.$$

1 Durch eine Permutation $\pi \in S_n$ der Spalten erhält man

$$\det \widetilde{A} = \frac{\varphi\big(a_{\pi(1)}, \dots, a_{\pi(n)}\big)}{\varphi(e_1, \dots, e_n)}.$$

Nach Lemma 9.4 gilt $\varphi(a_{\pi(1)}, \dots, a_{\pi(n)}) = \operatorname{sign} \pi \cdot \varphi(a_1, \dots, a_n)$. Daher folgt

$$\det \widetilde{A} = \operatorname{sign} \pi \cdot \frac{\varphi(a_1, \dots, a_n)}{\varphi(e_1, \dots, e_n)} = \operatorname{sign} \pi \cdot \det A.$$

2 Sei die Spalte a_i von A durch $a_i + \lambda \cdot a_j$ ersetzt. Nach Lemma 9.3 ist nun

$$\begin{aligned} \varphi(a_1, \dots, a_i + \lambda \cdot a_j, \dots, a_j, \dots, a_n) &= \varphi(a_1, \dots, a_i, \dots, a_j, \dots, a_n) \\ &+ \lambda \cdot \varphi(a_1, \dots, a_j, \dots, a_j, \dots, a_n) \\ &= \varphi(a_1, \dots, a_i, \dots, a_j, \dots, a_n). \end{aligned}$$

Es folgt

$$\det \widetilde{A} = \frac{\varphi(a_1, \dots, a_i + \lambda \cdot a_j, \dots, a_j, \dots, a_n)}{\varphi(e_1, \dots, e_n)} = \frac{\varphi(a_1, \dots, a_n)}{\varphi(e_1, \dots, e_n)} = \det A.$$

3 Man multipliziere die Spalte a_i mit $\lambda \in K$. Wegen

$$\varphi(a_1, \dots, \lambda \cdot a_i, \dots, a_n) = \lambda \cdot \varphi(a_1, \dots, a_i, \dots, a_n)$$

gilt dann

$$\det \widetilde{A} = \frac{\varphi(a_1, \ldots, \lambda \cdot a_i, \ldots, a_n)}{\varphi(e_1, \ldots, e_n)} = \lambda \cdot \frac{\varphi(a_1, \ldots, a_n)}{\varphi(e_1, \ldots, e_n)} = \lambda \cdot \det A.$$

4 Mit Korollar 9.11 und Lemma 9.9 folgt $\det A = 0 \iff \det \alpha = 0 \iff \alpha$ nicht invertierbar $\iff \alpha(e_1) = a_1, \ldots, \alpha(e_n) = a_n$ linear abhängig $\iff \operatorname{rang} A < n$.

5 Es ist $1_n = (a_{ij})$ mit $a_{ii} = 1$ und $a_{ij} = 0$ für $i \neq j$. Damit folgt $\det 1_n = \sum\limits_{\pi \in S_n} \operatorname{sign} \pi \cdot a_{1\pi(1)} \cdots a_{n\pi(n)} = \operatorname{sign} 1 \cdot a_{11} \cdots a_{nn} = 1$.

6 Sei $\beta : v \in K^n \longmapsto Bv$. Dann ist die lineare Abbildung $\alpha\beta : K^n \longrightarrow K^n$ durch $\alpha\beta(v) = \alpha\big(\beta(v)\big) = \alpha(Bv) = A(Bv) = (AB)v$ definiert. Mit Korollar 9.11 folgt $\det A \cdot \det B = \det \alpha \cdot \det \beta = \det \alpha\beta = \det AB$.

7 Die Aussage folgt aus $1 = \det 1_n = \det AA^{-1} = \det A \cdot \det A^{-1}$.

8 Es existiert eine invertierbare Matrix $T \in M_{n\times n}(K)$ mit $B = T^{-1}AT$. Daher folgt $\det B = \det T^{-1}AT = \det T^{-1} \cdot \det A \cdot \det T = \det T^{-1} \cdot \det T \cdot \det A = (\det T)^{-1} \cdot \det T \cdot \det A = \det A$.

Bemerkung

Satz 9.15 gibt an, wie sich die Determinante einer Matrix durch Anwendung des Gauß-Algorithmus ändert.

9.16 Satz

Sei $A = (a_{ij}) \in M_{n\times n}(K)$ eine obere Dreiecksmatrix, d.h. $a_{ij} = 0$ für $i > j$. Dann gilt $\det A = a_{11} \cdots a_{nn}$.

Beweis

Man betrachte $\det A = \sum\limits_{\pi \in S_n} \operatorname{sign} \pi \cdot a_{1\pi(1)} \cdots a_{n\pi(n)}$. Dabei ist ein Summand höchstens dann verschieden von 0, wenn $i \leq \pi(i)$ für alle $1 \leq i \leq n$ gilt. In diesem Fall folgt $n \leq \pi(n) \leq n \Longrightarrow n = \pi(n)$. Sukzessive erhält man $\pi = \mathrm{id}$, d.h. $\det A = \operatorname{sign} \mathrm{id} \cdot a_{11} \cdots a_{nn} = a_{11} \cdots a_{nn}$.

Beispiel

Für $a \neq 0$ gilt

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \det \begin{pmatrix} a & b \\ & d - ba^{-1}c \end{pmatrix} = a(d - ba^{-1}c) = ad - bc$$

und mit $a = 0$ gilt

$$\det \begin{pmatrix} & b \\ c & d \end{pmatrix} = -\det \begin{pmatrix} c & d \\ & b \end{pmatrix} = -cb = ad - bc.$$

Bemerkung

Sei $A_{ij} \in M_{m_i \times n_j}(K)$ für $1 \leq i \leq m$ und $1 \leq j \leq n$. Für $1 \leq j \leq p$ sei weiter $B_{jk} \in M_{n_j \times p_k}(K)$. Dann gilt $(A_{ij}) \cdot (B_{jk}) = (\sum\limits_{j=1}^{n} A_{ij} \cdot B_{jk})$.

Beweis

Man betrachte o.B.d.A.

$$A = \begin{pmatrix} A_{11} & \cdots & A_{1n} \end{pmatrix} \text{ und } B = \begin{pmatrix} B_{11} \\ \vdots \\ B_{n1} \end{pmatrix}$$

mit $A_{1j} \in M_{m \times n_j}(K)$ und $B_{j1} \in M_{n_j \times p}(K)$ für $1 \leq j \leq n$. Dann ist

$$A = \left(\begin{array}{ccc|c|ccc|c|ccc} a_{11} & \cdots & a_{1n_1} & \cdots & a_{1(s_j+1)} & \cdots & a_{1(s_j+n_j)} & \cdots & a_{1(s_n+1)} & \cdots & a_{1(s_n+n_n)} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn_1} & \cdots & a_{m(s_j+1)} & \cdots & a_{m(s_j+n_j)} & \cdots & a_{m(s_n+1)} & \cdots & a_{m(s_n+n_n)} \end{array}\right)$$

und

$$B = \left(\begin{array}{ccc} b_{11} & \cdots & b_{1p} \\ \vdots & \ddots & \vdots \\ b_{n_1 1} & \cdots & b_{n_1 p} \\ \hline \vdots & \ddots & \vdots \\ \hline b_{(s_j+1)1} & \cdots & b_{(s_j+1)p} \\ \vdots & \ddots & \vdots \\ b_{(s_j+n_j)1} & \cdots & b_{(s_j+n_j)p} \\ \hline \vdots & \ddots & \vdots \\ \hline b_{(s_n+1)1} & \cdots & b_{(s_n+1)p} \\ \vdots & \ddots & \vdots \\ b_{(s_n+n_n)1} & \cdots & b_{(s_n+n_n)p} \end{array}\right)$$

für $s_j = \sum\limits_{\lambda=1}^{j-1} n_\lambda$. Wegen

$$\begin{pmatrix} a_{1(s_j+1)} & \cdots & a_{1(s_j+n_j)} \\ \vdots & \ddots & \vdots \\ a_{m(s_j+1)} & \cdots & a_{m(s_j+n_j)} \end{pmatrix} \cdot \begin{pmatrix} b_{(s_j+1)1} & \cdots & b_{(s_j+1)p} \\ \vdots & \ddots & \vdots \\ b_{(s_j+n_j)1} & \cdots & b_{(s_j+n_j)p} \end{pmatrix}$$

$$= \begin{pmatrix} \sum\limits_{\mu=s_j+1}^{s_j+n_j} a_{1\mu}b_{\mu 1} & \cdots & \sum\limits_{\mu=s_j+1}^{s_j+n_j} a_{1\mu}b_{\mu p} \\ \vdots & \ddots & \vdots \\ \sum\limits_{\mu=s_j+1}^{s_j+n_j} a_{m\mu}b_{\mu 1} & \cdots & \sum\limits_{\mu=s_j+1}^{s_j+n_j} a_{m\mu}b_{\mu p} \end{pmatrix}$$

folgt

$$\sum_{j=1}^{n} A_{1j} \cdot B_{j1} = \sum_{j=1}^{n} \begin{pmatrix} \sum\limits_{\mu=s_j+1}^{s_j+n_j} a_{1\mu}b_{\mu 1} & \cdots & \sum\limits_{\mu=s_j+1}^{s_j+n_j} a_{1\mu}b_{\mu p} \\ \vdots & \ddots & \vdots \\ \sum\limits_{\mu=s_j+1}^{s_j+n_j} a_{m\mu}b_{\mu 1} & \cdots & \sum\limits_{\mu=s_j+1}^{s_j+n_j} a_{m\mu}b_{\mu p} \end{pmatrix}$$

und daher

$$\sum_{j=1}^{n} A_{1j} \cdot B_{j1} = \begin{pmatrix} \sum\limits_{\mu=1}^{n} a_{1\mu}b_{\mu 1} & \cdots & \sum\limits_{\mu=1}^{n} a_{1\mu}b_{\mu p} \\ \vdots & \ddots & \vdots \\ \sum\limits_{\mu=1}^{n} a_{m\mu}b_{\mu 1} & \cdots & \sum\limits_{\mu=1}^{n} a_{m\mu}b_{\mu p} \end{pmatrix} = A \cdot B.$$

9.17 Satz

Es sei durch $B \in M_{m\times m}(K)$ und $C \in M_{m\times n}(K)$ sowie $D \in M_{n\times n}(K)$ eine quadratische Matrix

$$A = \begin{pmatrix} B & C \\ & D \end{pmatrix}$$

gegeben. Dann gilt $\det A = \det B \cdot \det D$.

Beweis

Sei zunächst B nicht invertierbar, d.h. $\det B = 0$. Dann sind die Spalten b_i von B für $1 \leq i \leq m$ linear abhängig. Damit sind aber auch die entsprechenden Spalten

$$\begin{pmatrix} b_i \\ 0 \end{pmatrix}$$

von A linear abhängig. Also folgt $\det B \cdot \det C = 0 = \det A$.

Sei nun B invertierbar. Dann folgt

$$\begin{pmatrix} 1_m & \\ & D \end{pmatrix} \cdot \begin{pmatrix} B & \\ & 1_n \end{pmatrix} \cdot \begin{pmatrix} 1_m & B^{-1}C \\ & 1_n \end{pmatrix}$$

$$= \begin{pmatrix} B & \\ & D \end{pmatrix} \cdot \begin{pmatrix} 1_m & B^{-1}C \\ & 1_n \end{pmatrix}$$

$$= \begin{pmatrix} B & C \\ & D \end{pmatrix}.$$

Nach Satz 9.16 gilt

$$\det \begin{pmatrix} 1_m & B^{-1}C \\ & 1_n \end{pmatrix} = 1,$$

d.h. man erhält

$$\det \begin{pmatrix} B & C \\ & D \end{pmatrix} = \det \begin{pmatrix} 1_m & \\ & D \end{pmatrix} \cdot \det \begin{pmatrix} B & \\ & 1_n \end{pmatrix}.$$

Die Anwendung des Gauß-Algorithmus auf B bzw. D ist dabei analog zu seiner Anwendung auf

$$\begin{pmatrix} B & \\ & 1_n \end{pmatrix} \text{ bzw. } \begin{pmatrix} 1_m & \\ & D \end{pmatrix}.$$

Mit Satz 9.15 und Satz 9.16 folgt dann

$$\det B = \det \begin{pmatrix} B & \\ & 1_n \end{pmatrix} \text{ und } \det D = \det \begin{pmatrix} 1_m & \\ & D \end{pmatrix}.$$

Bemerkung

Satz 9.17 lässt sich nicht verallgemeinern, denn für Matrizen A, B, C und D gilt i.A.

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} \neq \det A \cdot \det D - \det B \cdot \det C.$$

9.18 Definition

Für $A = (a_{ij}) \in M_{n\times n}(K)$ sei $A'_{i,j} \in M_{n-1\times n-1}(K)$ die Matrix die durch Streichen der i-ten Zeile und j-ten Spalte aus A hervorgeht. Dann heißt $A_{ij} = (-1)^{i+j} \cdot \det A'_{i,j} \in K$ die Adjunkte von a_{ij}. Die Adjunkte der Matrix A ist $\operatorname{adj} A = (A_{ij})^t \in M_{n\times n}(K)$.

Beispiel

Sei $A \in K^{2\times 2}$ durch

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

gegeben. Dann ist $A_{11} = (-1)^2 \cdot \det(d) = d$, $A_{12} = (-1)^3 \cdot \det(c) = -c$, $A_{21} = (-1)^3 \cdot \det(b) = -b$ und $A_{22} = (-1)^4 \cdot \det(a) = a$. Damit gilt

$$\operatorname{adj} A = \begin{pmatrix} A_{11} & A_{21} \\ A_{12} & A_{22} \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

9.19 Satz (Laplacesche Entwicklungssatz)

Es sei $A = (a_{ij}) \in M_{n\times n}(K)$. Dann gilt $\det A = \sum\limits_{\lambda=1}^{n} a_{i\lambda} A_{i\lambda}$ für $1 \leq i \leq n$ (Entwicklung nach der i-ten Zeile) und $\det A = \sum\limits_{\lambda=1}^{n} a_{\lambda j} A_{\lambda j}$ für $1 \leq j \leq n$ (Entwicklung nach der j-ten Spalte).

Beweis

Sei zunächst $A^t = B = (b_{ij})$, d.h. $b_{ij} = a_{ji}$. Dann gilt $\det A = \det B$ und $\sum\limits_{j=1}^{n} a_{ij} A_{ij} = \sum\limits_{j=1}^{n} a_{ij} (-1)^{i+j} \cdot \det A'_{i,j} = \sum\limits_{j=1}^{n} b_{ji} (-1)^{j+i} \cdot \det B'_{j,i} = \sum\limits_{j=1}^{n} b_{ji} B_{ji}$. Daher ist lediglich $\det A = \sum\limits_{j=1}^{n} a_{ij} A_{ij}$ zu zeigen.

Sei nun $\alpha \in \operatorname{End}(K^n)$ definiert durch $\alpha(v) = Av$. Sei weiter $e_1, \ldots, e_n$ die Standardbasis von K^n und φ eine nicht ausgeartete, alternierende n-Linearform auf K^n. Dann gilt

$$\det A = \det \alpha = \frac{\varphi\big(\alpha(e_1), \ldots, \alpha(e_n)\big)}{\varphi(e_1, \ldots, e_n)}.$$

Dabei liefert $\alpha(e_j)$ die j-te Spalte von A, d.h. $\alpha(e_j) = \sum\limits_{i=1}^{n} a_{ij} e_i$. Es folgt

$$\begin{aligned} \det A &= \frac{\varphi\Big(\alpha(e_1), \ldots, \alpha(e_{j-1}), \sum\limits_{i=1}^{n} a_{ij} e_i, \alpha(e_{j+1}), \alpha(e_n)\Big)}{\varphi(e_1, \ldots, e_n)} \\ &= \sum_{i=1}^{n} a_{ij} \frac{\varphi\Big(\alpha(e_1), \ldots, \alpha(e_{j-1}), e_i, \alpha(e_{j+1}), \alpha(e_n)\Big)}{\varphi(e_1, \ldots, e_n)}. \end{aligned}$$

Sei nun $\beta_i : v \in K^n \longmapsto B_i v$ durch

$$B_i = \begin{pmatrix} a_{11} & \cdots & a_{1j-1} & 0 & a_{1j+1} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{i-11} & \cdots & a_{i-1j-1} & 0 & a_{i-1j+1} & \cdots & a_{i-1n} \\ a_{i1} & \cdots & a_{ij-1} & 1 & a_{ij+1} & \cdots & a_{in} \\ a_{i+11} & \cdots & a_{i+1j-1} & 0 & a_{i+1j+1} & \cdots & a_{i+1n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nj-1} & 0 & a_{nj+1} & \cdots & a_{nn} \end{pmatrix}$$

definiert. Dann gilt $\beta_i(e_k) = B_i e_k = A_i e_k = \alpha(e_k)$ für $1 \leq k \leq n$ mit $k \neq j$ und $\beta_i(e_j) = B_i e_j = e_i$. Man erhält also

$$\frac{\varphi\big(\alpha(e_1), \ldots, \alpha(e_{j-1}), e_i, \alpha(e_{j+1}), \alpha(e_n)\big)}{\varphi(e_1, \ldots, e_n)} = \frac{\varphi\big(\beta_i(e_1), \ldots, \beta_i(e_n)\big)}{\varphi(e_1, \ldots, e_n)} = \det B_i$$

für $1 \leq i \leq n$, d.h.

$$\det A = \sum_{i=1}^{n} a_{ij} \det B_i.$$

Durch $j-1$ Spaltenvertauschungen und $i-1$ Zeilenvertauschungen angewandt auf B_i erhält man dann

$$N_{ij} = \begin{pmatrix} 1 & a_{i1} & \cdots & a_{ij-1} & a_{ij+1} & \cdots & a_{in} \\ 0 & a_{11} & \cdots & a_{1j-1} & a_{1j+1} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_{i-11} & \cdots & a_{i-1j-1} & a_{i-1j+1} & \cdots & a_{i-1n} \\ 0 & a_{i+11} & \cdots & a_{i+1j-1} & a_{i+1j+1} & \cdots & a_{i+1n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n1} & \cdots & a_{nj-1} & a_{nj+1} & \cdots & a_{nn} \end{pmatrix}.$$

Nach Satz 9.15 gilt dabei $\det N_{ij} = (-1)^{i-1} \cdot (-1)^{j-1} \cdot \det B_i = (-1)^{i+j-2} \cdot \det B_i$, also $\det B_i = (-1)^{i+j} \cdot \det N_{ij}$. Nach Satz 9.17 folgt wegen

$$N_{ij} = \begin{pmatrix} 1 & a_{i1} & \cdots & a_{ij-1} & a_{ij+1} & \cdots & a_{in} \\ 0 & & & & & & \\ \vdots & & & A'_{i,j} & & & \\ 0 & & & & & & \end{pmatrix}$$

schließlich $\det N_{ij} = \det A'_{i,j}$. Insgesamt ist also

$$\det A = \sum_{i=1}^{n} a_{ij} \cdot (-1)^{i+j} \cdot \det A'_{i,j} = \sum_{i=1}^{n} a_{ij} A_{ij}.$$

Beispiel

Es sei

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & & 5 \\ 6 & & 7 \end{pmatrix}$$

gegeben. Dann gilt $\det A = 2 \cdot A_{12} + 0 \cdot A_{22} + 0 \cdot A_{32} = 2 \cdot (-1)^{1+2} \cdot \det A'_{1,2}$ mit

$$\det A'_{1,2} = \det \begin{pmatrix} 4 & 5 \\ 6 & 7 \end{pmatrix} = 4 \cdot 7 - 5 \cdot 6 = -2.$$

Also ist $\det A = 4$.

9.20 Satz

Sei eine quadratische Matrix $A = (a_{ij}) \in M_{n \times n}(K)$ gegeben. Dann gilt $A \cdot \operatorname{adj} A = \operatorname{adj} A \cdot A = (\det A) \cdot 1_n$. Falls A invertierbar ist, gilt insbesondere $A^{-1} = (\det A)^{-1} \cdot \operatorname{adj} A$.

Beweis

Man betrachte $(b_{ij}) = \operatorname{adj} A = (A_{ij})^t$, also $b_{ji} = A_{ij}$. Dann gilt $A \cdot \operatorname{adj} A = (a_{ik}) \cdot (b_{kj}) = (\sum\limits_{k=1}^{n} a_{ik} b_{kj}) = (\sum\limits_{k=1}^{n} a_{ik} A_{jk})$.

Sei nun $C = (c_{ij})$ die Matrix, die aus A entsteht, indem man die j-te Zeile durch die i-te Zeile ersetzt. Dann gilt $c_{jk} = c_{ik} = a_{ik}$ und $A'_{j,k} = C'_{j,k}$ – also $A_{jk} = (-1)^{j+k} \cdot \det A'_{j,k} = (-1)^{j+k} \cdot \det C'_{j,k} = C_{jk}$ – für $1 \leq k \leq n$. Mit Satz 9.19 folgt $\sum\limits_{k=1}^{n} a_{ik} A_{jk} = \sum\limits_{k=1}^{n} c_{jk} C_{jk} = \det C$.

Für $i \neq j$ stimmen aber in C zwei Zeilen überein, d.h. $\sum\limits_{k=1}^{n} a_{ik} A_{jk} = \det C = 0$. Für $i = j$ gilt $\sum\limits_{k=1}^{n} a_{ik} A_{ik} = \det A$. Insgesamt gilt also $A \cdot \operatorname{adj} A = (\sum\limits_{k=1}^{n} a_{ik} A_{jk}) = \det A \cdot 1_n$. Analog folgt $\operatorname{adj} A \cdot A = (\det A) \cdot 1_n$.

9.21 Korollar (Cramersche Regel)

Sei $A \in M_{n \times n}$ invertierbar und $b \in K^n$. Dann hat das lineare Gleichungssystem $Ax = b$ die eindeutige Lösung $\mathring{x} \in K^n$ mit $\mathring{x}_j = (\det A)^{-1} \cdot \sum\limits_{i=1}^{n} b_i A_{ij}$.

Beweis

Da A invertierbar ist, hat $Ax = b$ die Lösung $\mathring{x} = A^{-1}b$. Weiter hat $Ax = 0$ nach Satz 8.5 die eindeutige Lösung $x = 0$. Nach Satz 8.4 gilt für die Lösungsmenge L von $Ax = b$ also $L = \mathring{x} + \{0\} = \{\mathring{x}\}$.

Nach Satz 9.20 gilt nun $\mathring{x} = A^{-1}b = (\det A)^{-1} \cdot (\operatorname{adj} A) \cdot b$. Mit $(c_{ij}) = C = (\operatorname{adj} A) = (A_{ij})^t$ – also $c_{ij} = A_{ji}$ – gilt dann $\mathring{x}_j = (\det A)^{-1} \cdot \sum\limits_{i=1}^{n} c_{ji} b_i = \sum\limits_{i=1}^{n} b_i A_{ij}$.

10 Eigenwerte und Eigenvektoren

10.1 Definition

Sei α ein Endomorphismus eines K-Vektorraums V. Ein Vektor $v \in V \setminus \{0\}$ heißt Eigenvektor, wenn ein $\lambda \in K$ mit $\alpha(v) = \lambda v$ existiert. Ein Eigenvektor $v \in K^n \setminus \{0\}$ einer quadratischen Matrix $A \in M_{n \times n}(K)$ ist ein Eigenvektor der linearen Abbildung $v \longmapsto Av$. Ein Skalar $\lambda \in K$ mit $0 \neq v \longmapsto \lambda v$ heißt Eigenwert.

Beispiel

Sei $\alpha : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ durch

$$\alpha \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2x + 3y \\ 4y \end{pmatrix}$$

definiert. Dann ist

$$v = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

ein Eigenvektor zu dem Eigenwert $\lambda = 2$.

Bemerkung

Die Eigenvektoren $v \in V$ eines Endomorphismus α zu dem Eigenwert $\lambda = 0$ sind genau die Elemente $v \in \operatorname{Kern} \alpha \setminus \{0\}$.

10.2 Satz

Seien $v_1, \ldots, v_m$ Eigenvektoren eines Endomorphismus $\alpha : V \longrightarrow V$ zu paarweise verschiedenen Eigenwerten. Dann sind $v_1, \ldots, v_m$ linear unabhängig.

Beweis

Wir zeigen die Aussage durch vollständige Induktion über m. Für $m = 1$ erhält man einen Eigenvektor $v_1 \in V$. Wegen $v_1 \neq 0$ ist dann $\{v_1\}$ linear unabhängig.

Nun betrachte man die Linearkombination

$$\sum_{i=1}^{m} \mu_i v_i = 0$$

für Eigenvektoren $v_1, \ldots, v_m$ mit paarweise verschiedenen Eigenwerten $\lambda_1, \ldots, \lambda_m$. Dann gilt auch

$$\sum_{i=1}^{m} \lambda_1 \mu_i v_i = \lambda_1 \sum_{i=1}^{m} \mu_i v_i = \lambda_1 \cdot 0 = 0$$

und

$$0 = \alpha(0) = \alpha(\sum_{i=1}^{m} \mu_i v_i) = \sum_{i=1}^{m} \mu_i \alpha(v_i) = \sum_{i=1}^{m} \mu_i \lambda_i v_i.$$

Es folgt

$$0 = \sum_{i=1}^{m} \mu_i \lambda_i v_i - \sum_{i=1}^{m} \lambda_1 \mu_i v_i = \sum_{i=2}^{m} \mu_i (\lambda_i - \lambda_1) v_i$$

Da nach Induktionsannahme $v_2, \ldots, v_m$ linear unabhängig sind, erhält man $\mu_i(\lambda_i - \lambda_1) = 0$ für $2 \leq i \leq m$. Wegen $\lambda_1 \neq \lambda_i \Longleftrightarrow \lambda_i - \lambda_1 \neq 0$ gilt $\mu_i = 0$ für $2 \leq i \leq m$, d.h. es bleibt $\mu_1 v_1 = 0$. Da aber v_1 ein Eigenvektor ist, folgt $v_1 \neq 0 \Longrightarrow \mu_1 = 0$. Insgesamt sind also $v_1, \ldots, v_m$ linear abhängig.

Bemerkung

Die Umkehrung von Satz 10.2 gilt i.A. nicht. Etwa ist für $\mathrm{id} : V \longrightarrow V$ jeder Vektor $v \in V$ – also insbesondere jedes Element einer linear unabhängigen Teilmenge $M \subseteq V$ – ein Eigenvektor mit Eigenwert $\lambda = 1$.

10.3 Definition / Bemerkung

Sei $\alpha : V \longrightarrow V$ ein Endomorphismus und $\lambda \in K$ ein Eigenwert von α. Dann ist $E_\lambda = \{v \in V \mid \alpha(v) = \lambda \cdot v\} = \mathrm{Kern}(\alpha - \lambda \cdot \mathrm{id})$ ein Unterraum und wird als Eigenraum von $\lambda \in K$ bezeichnet. Die Dimension des Eigenraums E_λ ist die geometrische Vielfachheit des Eigenwerts λ.

10.4 Definition

Für $A = (A_{ij}) \in M_{n\times n}(K)$ ist

$$\chi_A(x) = \det(x \cdot 1_n - A) = \det \begin{pmatrix} x - a_{11} & \cdots & -a_{1n} \\ \vdots & \ddots & \vdots \\ -a_{n1} & \cdots & x - a_{nn} \end{pmatrix}$$

das charakteristische Polynom.

10.5 Satz

Sei $A \in M_{n\times n}(K)$. Dann ist $\chi_A(x)$ ein normiertes Polynom vom Grad n, d.h. $\chi_A(x) = x^n + A_1 x^{n-1} + \ldots + A_n$ für $A_i \in K$. Ferner ist $\lambda \in K$ genau dann ein Eigenwert von A, wenn $\chi_A(\lambda) = 0$ gilt.

Beweis

Es sei $(b_{ij}) = x \cdot 1_n - A$, d.h. $b_{ii} = x - a_{ii}$ und $b_{ij} = -a_{ij}$ für $i \neq j$. Dann gilt

$$\chi_A(x) = \det B = \sum_{\pi \in S_n} \operatorname{sign} \pi \cdot b_{1\pi(1)} \cdots b_{n\pi(n)}.$$

Jeder Summand $\operatorname{sign} \pi \cdot b_{1\pi(1)} \cdots b_{n\pi(n)}$ mit $\pi \neq 1$ ist dabei ein Polynom vom Grad $m_\pi < n$. Also folgt

$$\chi_A(x) = \operatorname{sign} 1 \cdot b_{11} \cdots b_{nn} + \sum_{\pi \neq 1} \operatorname{sign} \pi \cdot b_{1\pi(1)} \cdots b_{n\pi(n)} = (x - a_{11}) \cdots (x - a_{nn}) + p$$

für ein Polynom p mit Grad $m < n$. Damit ist $\chi_A(x)$ ein normiertes Polynom vom Grad n.

Für $\lambda \in K$ betrachte man $\beta : v \in K^n \longmapsto (\lambda \cdot 1_n - A)v$. Nach Korollar 9.11 gilt $\det \beta \neq 0$ genau dann, wenn β invertierbar ist. Dies ist nach Korollar 7.6 genau dann der Fall, wenn β injektiv ist. Nach Lemma 7.3 ist dies äquivalent zu $\operatorname{Kern} \beta = \{0\}$. Da nach Satz 9.14 nun $\det \beta = \det(\lambda \cdot 1_n - A) = \chi_A(\lambda)$ gilt, folgt also

$$\chi_A(\lambda) = 0 \Longleftrightarrow \exists\ 0 \neq v \text{ mit } (\lambda \cdot 1_n - A)v = 0.$$

Wegen $(\lambda \cdot 1_n - A)v = 0 \Longleftrightarrow \lambda v = Av$ ist also λ genau dann ein Eigenwert, wenn $\chi_A(\lambda) = 0$ gilt.

Bemerkung

Das konstante Glied des charakteristischen Polynoms $\chi_A(x)$ einer Matrix $A \in M_{n\times n}(K)$ ist $\chi_A(0) = \det(-A) = (-1)^n \cdot \det A$.

Beispiel

Es sei die Matrix
$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
gegeben. Dann gilt
$$\chi_A(x) = \det \begin{pmatrix} x-a & -b \\ -c & x-d \end{pmatrix} = (x-a)(x-d) - bc = x^2 - (a+d)x + ad - bc$$
mit $ad - bc = \det A$.

10.6 Lemma

Die charakteristischen Polynome ähnlicher Matrizen stimmen überein.

Beweis

Seien $A, B \in M_{n\times n}(K)$ mit $B = T^{-1}AT$ für eine invertierbare Matrix $T \in M_{n\times n}(K)$. Dann gilt $\chi_B(x) = \det(x \cdot 1_n - B) = \det(x \cdot T^{-1}T - T^{-1}AT) = \det(T^{-1}xT \cdot -T^{-1}AT) = \det T^{-1}(x \cdot 1_n - A)T$. Mit Satz 9.15 folgt $\chi_B(x) = \det T^{-1}(x \cdot 1_n - A)T = \det(x \cdot 1_n - A) = \chi_A(x)$.

10.7 Definition / Bemerkung

Sei $\alpha \in \mathrm{End}(V)$ bzgl. einer endlichen Basis B von V durch $A = M_\alpha(B, B)$ dargestellt. Dann ist $\chi_\alpha(x) = \chi_A(x)$ das charakteristische Polynom von α. Dabei ist $\chi_\alpha(x)$ wohldefiniert.

Beweis

Sei α bzgl. einer weiteren Basis $\widetilde{B}$ von V durch $\widetilde{A} = M_\alpha(\widetilde{B}, \widetilde{B})$ dargestellt. Nach Korollar 7.12 sind dann A und $\widetilde{A}$ ähnlich. Mit Lemma 10.6 gilt also $\chi_A(x) = \chi_{\widetilde{A}}(x)$.

10.8 Definition

Ein Körper K heißt algebraisch abgeschlossen, wenn jedes Polynom $f(x) = a_0 + a_1x + \ldots + a_nx^n$ mit $n \geq 1$ und $a_n \neq 0$ eine Nullstelle in K hat.

Beispiel

Für alle $x \in \mathbb{R}$ gilt $x^2 + 1 \geq 1$, d.h. $\mathbb{R}$ ist nicht algbraisch abgeschlossen.

Bemerkung

Nach dem „Fundamentalsatz der Algebra“ ist $\mathbb{C}$ algebraisch abgeschlossen.

10.9 Satz

Matrizen über algebraisch abgeschlossenen Körpern besitzen stets Eigenwerte.

Beweis

Nach Satz 10.5 ist das charakteristische Polynom $\chi_A(x)$ einer Matrix $A \in M_{n\times n}(K)$ ein Polynom vom Grad $n \geq 1$. Daher besitzt $\chi_A(x)$ in einem algebraisch abgeschlossenen Körper mindestens eine Nullstelle. Diese Nullstelle ist dann ein Eigenwert von A.