Lineare Algebra 1

[MAT.103UF]

gelesen von: Franz Lehner, Assoc.Prof. Dipl.-Ing. Dr.
am Institut für Diskrete Mathematik

Verfasst von: Moritz Mossböck
11820925
moritz.mossboeck@student.tugraz.at

Wintersemester 2021/22

Inhaltsverzeichnis

Was ist Lineare Algebra?

Wir können die Mathematik grob in verschiedene Teilgebiete aufteilen:

- Arithmetik (gr. $\alpha\rho\iota\vartheta\mu\eta\tau\iota\kappa\eta$), das Rechnen mit Zahlen
- Geometrie (gr. $\gamma\varepsilon o\mu\varepsilon\tau\rho\iota\alpha$)
- Analysis (gr. $\alpha\nu\alpha\lambda\upsilon\sigma\iota\varsigma$), die Infinitesemalrechnung
- Algebra, das Rechnen mit Symbolen und Strukturen

In der linearen Algebra werden wir uns speziell mit dem Rechnen mit **Vektoren** und **Matrizen** bzw. eigentlich **Vektorräumen** und **linearen Abbildungen** beschäftigen. Dazu müssen wir uns jedoch ein gewisses Fundament an Basiswissen aufbauen, beginnend mit drei elementaren Begriffen, die jeder Mathematiker kennen und verstehen sollte:

- Definition
- Satz
- Beweis

Definitionen sind im Sinne der Mathematik (nach den **Axiomen**) die grundlegendsten Festlegungen, welche verwendet werden, um Sätze zu formulieren. Eine Definition ist somit etwas, das einen Begriff bzw. ein Objekt klar abgrenzt, benennt und, sofern nötig, etwas Symbolik festlegt.

Sätze sind Aussagen, die eine Behauptung aufstellen. Ein klassisches Beispiel ist etwa der Satz des Pythagoras, welcher die Katheten eines rechtwinkeligen Dreiecks mit der zugehörigen Hypotenuse in Verbindung setzt. Damit ein Satz tatsächlich verwendet werden kann, muss erst gezeigt werden, dass man ihn verwenden darf, und zwar in allen möglichen Fällen.

Um so etwas zu zeigen, wird im Allgemeinen ein Beweis geführt. Beweise bestehen aus einer Kette "logischer Schlussfolgerungen", welche nur auf Axiomen und Definitionen basieren, um die Implikation eines Satzes unumstößlich nachzuweisen. Beweise sind insofern komplex, da es kein allgemeines Schema gibt, um einen beliebigen Satz zu beweisen. Es erfordert oftmals viel Zeit und Kreativität, um einen Satz zu beweisen.

A	α	Alpha	N	ν	Ny
B	β	Beta	Ξ	ξ	Xi
Γ	γ	Gamma	O	o	Omikron
Δ	δ	Delta	Π	π	Pi
E	ϵ, ε	Epsilon	P	ρ	Rho
Z	ζ	Zeta	Σ	σ, ς	Sigma
H	η	Eta	T	τ	Tau
Θ	θ, ϑ	Theta	Υ	υ	Ypsilon
I	ι	Iota	Φ	ϕ, φ	Phi
K	κ	Kappa	X	χ	Chi
Λ	λ	Lambda	Ψ	ψ	Psi
M	μ	My	Ω	ω	Omega

Tabelle 1: Das griechische Alphabet

Zusätzlich zu den griechischen Buchstaben, von denen wir meistens die kleinen verwenden werden, wird oftmals noch der erste hebräische Buchstabe $\aleph$ (lies: aleph) verwendet. Mit $\aleph_0$ bezeichnet man im Allgemeinen die Größe der natürlichen Zahlen.

1 Mengen, Vektoren und lineare Gleichungssysteme

Wir beginnen mit einer Vereinbarung, da wir uns in dieser Vorlesung nicht direkt mit einer exakten Definition des Mengenbegriffes auseinandersetzen wollen.

Bemerkung 1.1: Mengenbegriff nach CANTOR

Unter einer Menge verstehen wir jede Zusammenfassung M von bestimmten, wohlunterschiedenen Objekten unserer Anschauung, oder unseres Denkens zu einem Ganzen.

Diese Vereinbarung mag auf den ersten Blick simpel und "logisch" wirken, birgt aber doch einige Ungereimtheiten. Bertrand RUSSEL etwas, hat einen entscheidenden Widerspruch in der Cantor'schen Mengenlehre entdeckt, welcher sich nicht beheben lässt und auf ein nicht-entscheidbares Problem führt.

Bevor wir uns aber diesem Problem widmen, müssen wir erst etwas Notation festlegen. Sei M eine Menge, also eine Ansammlung von wohlunterschiedenen Objekten, so trifft für ein beliebiges Objekt x genau eines zu:

- x ist in M enthalten, $x \in M$
- x ist nicht in M enthalten, $x \notin M$

Gilt $x \in M$ so bezeichnen wir x als ein Element von M. Um zu prüfen, ob ein Objekt ein Element einer Menge ist, müssen wir erst festlegen, aus welchen Elementen die Menge besteht. Dazu gibt es zwei Methoden: die Aufzählung aller Elemente in der Menge, oder die Beschreibung der Elemente durch eine Aussageform. Wird eine Menge aufzählend festgelegt, so muss jedes Element aufgelistet werden. Das kann unter Umständen ein ziemlicher Aufwand sein, kann für "kleine" Mengen aber auch eine gute Basis zum besseren Verständnis liefern.

$$\begin{aligned} M &= \{1, 2, 3\} \\ M &= \{\text{a}, \text{b}, \text{Teddybär}, \text{HS } 62.01, \{1, 2, 3\}\} \\ M &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} = \{1, 2, \dots, 10\} \\ \mathbb{N} &= \{1, 2, \dots\} \end{aligned}$$

Wir sehen bei der dritten Menge, dass wir die Aufzählung auch verkürzen können. Auch die natürlichen Zahlen $\mathbb{N}$ kann man so festlegen. Allerdings ist diese Notation nicht immer eindeutig:

$$\begin{aligned} M &= \{1, 4, 9, \dots\} \\ M &= \{2, 3, 5, 7, 11, \dots\} \\ M &= \{2, 3, 45, \dots\} \end{aligned}$$

Obwohl für alle dieser drei Mengen relativ gut erkennbare Muster bzw. Regeln gibt, wie sie fortzusetzen sind, ist diese Methode, eine Menge festzulegen nicht eindeutig. Man könne genauso gut $M = \{1, 4, 9, 15, \dots\}$ schreiben, und nicht so schnell bzw. gar kein Muster finden. Um Verwirrung bei "größeren" Mengen zu vermeiden, verwendet man eine Aussageform, um die Elemente anhand ihrer Eigenschaften zu bestimmen:

$$\begin{aligned} M &= \{n \colon n \text{ ist das Quadrat einer natürlichen Zahl}\} \\ &= \{n \colon \text{es gibt } k \in \mathbb{N}, \text{sodass } n = k^2\} \\ &= \{n \colon \exists k \in \mathbb{N} \colon n = k^2\} \\ &= \{k^2 \colon k \in \mathbb{N}\} \end{aligned}$$

Die Beschreibung der Elemente über ihre Eigenschaften ist insofern sinnvoll, wenn man z.B. mit Mengen arbeitet, welche überabzählbar sind, wie etwa die reellen Zahlen $\mathbb{R}$. Zusätzlich ist diese Notation kompakt und gibt Einsicht, warum gewisse Objekte Elemente einer Menge sind. Einige wichtige Mengen, die oftmals verwendet werden sind:

- $\mathbb{N} = \{1, 2, 3, 4, \dots\}$, die natürlichen Zahlen
- $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$, die natürlichen Zahlen mit 0
- $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$, die ganzen Zahlen
- $\mathbb{Q} = \left\{ \frac{p}{q} \colon p \in \mathbb{Z}, q \in \mathbb{N} \right\}$, die rationalen Zahlen

- $\mathbb{R}$, die reellen Zahlen

Die reellen Zahlen sind nicht ganz so leicht zu definieren, wie etwas die rationalen Zahlen. Sie beinhalten nebst rationalen Zahlen auch **irrationalen Zahlen**, wie etwa $\sqrt{2}$, π, e et cetera. Diese Zahlen können nicht mit "herkömmlichen" Methoden beschrieben werden, sondern sind oftmals durch Grenzwertprozesse definiert. Eine interessante Ansammlung an reellen Zahlen ist die Menge der algebraischen Zahlen. Eine algebraische Zahl ist die Lösung einer Polynomgleichung $a_0 + a_1 x + \cdots + a_n x^n = 0$, wobei die Koeffizienten rationale Zahlen sind.

Der Begriff der reellen Zahlen wurde erstmals von Richard DEDEKIND ernsthaft untersucht. Etwa zur gleichen Zeit tauchte ein großes Problem auf: die Kontinuumshypothese. Diese Hypothese beschäftigte sich mit der Frage, ob zwischen $|\mathbb{N}|$ und $|\mathbb{R}|$ noch eine weitere Menge war. Es stellt sich heraus, dass dieses Problem nicht entscheidbar ist. Es gibt Systeme der Mathematik, in denen existiert etwas dazwischen, und es gibt Systeme, wo dem nicht so ist.

Zuletzt betrachten wir die komplexen Zahlen $\mathbb{C}$. Diese Zahlenmenge tauchte im Zusammenhang mit der Untersuchung der Lösbarkeit von Polynomgleichungen auf. Nach Carl Friedrich GAUSS, hat die folgende Gleichung exakt zwei Lösungen:

$$x^2 + 2 = 0$$

Formen wir jedoch die Gleichung um, so sehen wir schnell, dass $x^2 = -2$ gelten muss. Das ist in den reellen Zahlen nicht möglich. Daher wurde nach einigen Durchbrüchen im Denkwesen der Mathematik die imaginäre Einheit i eingeführt, mit welcher die komplexen Zahlen definiert sind:

$$\mathbb{C} = \{a + \mathrm{i}b : a, b \in \mathbb{R}, \mathrm{i}^2 = -1\}$$

Eine weitere wichtige Menge ist die leere Menge $\emptyset = \{\}$. Sie enthält keine Elemente. Es sieht so aus, als könnte $\emptyset$ nicht wirklich eine Menge sein, da wir ja voraussetzen, dass eine Menge eine Ansammlung von Elementen ist. Daher müssen wir ein Axiom verwenden, welches besagt, dass die leere Menge existiert.

1.1 Konstruktionen

Nachdem wir nun in Grundzügen Mengen eingeführt haben, wollen wir untersuchen, wie man mit Mengen arbeiten kann. Dazu legen wir zuerst den Begriff der Teilmenge fest. Seien A und B Mengen, so ist A eine Teilmenge von B, wenn jedes Element von A auch in B enthalten ist. Wir schreiben dann $A \subseteq B$. Diese Version einer Teilmenge schließt die Gleichheit von A und B nicht aus. Will man explizit erwähnen, dass A ungleich zu B ist, so schreibt man oftmals $A \subset B$.

$$\mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

Die leere Menge $\emptyset$ ist Teilmenge jeder Menge. Dieser Umstand wirkt vielleicht widersprüchlich, da $\emptyset$ keine Elemente hat, aber genau deswegen wird sie als Teilmenge jeder Menge betrachtet.

Die erste Operation, die wir untersuchen ist der **Durchschnitt** von zwei Mengen A und B, $A \cap B$. Wie der Name verrät, ist der Durchschnitt jene Menge, deren Elemente sowohl in A als auch in B enthalten sind:

$$A \cap B = \{x \colon x \in A \wedge x \in B\}$$

Die zweite Operation ist die **Vereinigung** zweier Mengen A und B, $A \cup B$. Die Vereinigung ist jede Menge, deren Elemente in A oder[1] in B enthalten sind:

$$A \cup B = \{x \colon x \in A \vee x \in B\}$$

Zuletzt wollen wir noch A ohne B betrachten, also die Menge aller Elemente in A, die nicht in B enthalten sind. Wir schreiben $A \setminus B$:

$$A \setminus B = \{x \colon x \in A \wedge x \notin B\}$$

Wir können diese drei Operationen schön mit **Venn-Diagrammen** darstellen:

[1] hierbei handelt es sich um ein inklusives Oder, sprich die Elemente können auch in A und B enthalten sein

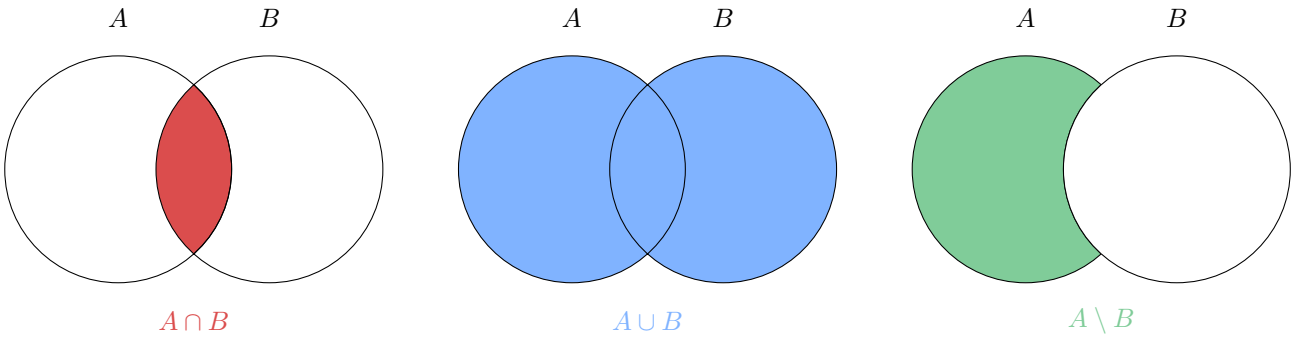

Abbildung 1: Graphische Veranschaulichung des Durchschnitts (links), der Vereinigung (mitte) und von A ohne B (rechts)

Sofern wir keine Grundmenge X vorgeben, mit $A \subseteq X$, können wir keine "größte Menge" festlegen. Allerdings ist es immer Möglich die "kleinste" Menge zu finden, nämlich die leere Menge. Wenn A Teilmenge einer Grundmenge X ist, so können wir das Komplement von A bezüglich X bilden:

$$A^c = X \setminus A = \{x \in X : x \notin A\}$$

Zuletzt wollen wir die **Potenzmenge** einer Menge untersuchen. Die Potenzmenge $\mathcal{P}(M)$ einer Menge M ist die Menge aller Teilmengen von M:

$$\mathcal{P}(M) = \{N : N \subseteq M\}$$

Die Potenzmenge einer endlichen Menge M mit n Elementen hat genau 2^n Elemente, inklusive der Menge M.

1.2 Lineare Gleichungssysteme

Ein lineares Gleichungssystem ist ein System von Gleichungen der folgenden Gestalt:

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

Wir haben hier m Gleichungen in n Unbekannten mit reellen Koeffizienten $a_{ij} \in R$ mit $i = 1, \ldots m$ und $j = 1, \ldots n$ und reellen Zahlen $b_i \in \mathbb{R}$. Wir wollen die Lösungen dieses Systems finden, wir suchen also ein n-Tupel $(x_1, x_2, \ldots, x_n)$ mit reellen Zahlen x_j, sodass alle Gleichungen erfüllt sind.

Tupel sind eine spezielle Art "Menge", in denen die Anzahl der Reihenfolge der Elemente eine Rolle spielt. So ist etwas $(1, 2)$ nicht gleich $(2, 1)$. Bei normalen Mengen gilt hingegen $\{1, 2\} = \{2, 1\}$. Tupel mit n Einträgen werden allgemein als n-Tupel beschrieben. Hingegen wird ein Tupel mit nur einem Element (x_1) als **Zahl**[2] bezeichnet. Ein Tupel mit zwei Elementen (x_1, x_2) als Paar, dreielementige Tupel (x_1, x_2, x_3) heißen Tripel. Weiters kann man Quadrupel, Quintupel, Sextupel, et cetera verwenden, allerdings sagt man oft auch einfach 4-Tupel, 5-Tupel usw.

Betrachten wir zunächst den Fall $y = kx + d$. Wir wollen herausfinden, für welche x die Bedingung $y = 0$ erfüllt ist. Dazu führen wir einfach Äquivalenzumformungen aus:

$$kx + d = 0 \Leftrightarrow kx = -d \Leftrightarrow x = -\frac{d}{k}$$

Hier müssen wir darauf achten, dass k nicht 0 sein darf. Das macht insofern Sinn, da für $y = d, d \neq 0$ der Graph nie die x-Achse schneidet, also keine Lösungen existieren. Anders verhält es sich, wenn $d = 0$ ist. Dann

[2] später auch **Skalar**

gibt es nämlich unendlich viele Lösungen, da $0 \cdot x + 0$ immer 0 ist, die Gleichung also immer erfüllt. In unserer allgemeinen Schreibweise können wir $kx + d = 0$ folgendermaßen festlegen:

$$ax = b \Leftrightarrow x = \frac{b}{a}, a \neq 0$$

Wie bereits erwähnt müssen wir für $a = 0$ eine Fallunterscheidung machen, ob $b = 0$ oder $b \neq 0$. Um Lineare Gleichungssystem kompakt anzuschreiben verwenden wir eine **Matrix**. Dabei handelt es sich um ein rechteckiges Zahlenschema mit n Spalten und m Zeilen. Wir können die Koeffizienten unseres Systems in einer Matrix festhalten:

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

Prinzipiell macht es Sinn, die Matrix des Gleichungssystems um eine weiter Spalte zu erweitern, um alle b_i festzuhalten. Das hat später den Vorteil, wenn wir Lösungsverfahren anwenden, dass wir gleiche die gesamte Gleichung verändern und nicht separat die b_i bearbeiten müssen:

$$\left[\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right]$$

Wir nennen diese Matrix die **erweiterte Koeffizientenmatrix**. Für den Fall, dass $b_i = 0$, nennen wir das System **homogen**. In diesem Fall ist das n-Tupel $(0, 0, \ldots, 0)$ immer eine (triviale) Lösung.

Wir haben nun bereits den Fall $m = n = 1$ untersucht. Wie verhält es sich mit $m = 1$ und $n = 2$? Wir erhalten eine Gleichung mit 2 Unbekannten x und y:

$$a_1 x + a_2 y = b \Leftrightarrow y = -\frac{a_1}{a_2} x + \frac{b}{a_2}$$

Hierbei handelt es sich um eine Gerade in $\mathbb{R}^2$, wir haben also unendlich viele Lösungen, da wir zu jedem x ein passendes y finden können, sofern $a_2 \neq 0$. Unsere Lösungsmenge ist also $L = \{(x, y) \colon a_1 x + a_2 y = b\}$ bzw.:

$$L = \left\{ \left(x, -\frac{a_1}{a_2} x + \frac{b}{a_2} \right) | x \in \mathbb{R} \right\}$$

Wir müssen nun noch den Sonderfall $a_2 = 0$ untersuchen. In diesem Fall reduziert sich das Problem auf $a_1 x = b$, welches wir bereits behandelt haben. Weiters interessiert uns der Fall $m = n = 2$. Wir betrachten also ein System der folgenden Form:

$$\begin{aligned} a_{11} x + a_{12} y &= b_1 \\ a_{21} x + a_{22} y &= b_2 \end{aligned}$$

Für diesen Fall (wie für die bisherigen auch) können wir das Problem geometrisch Darstellen. Da jede Gleichung eine Gerade in $\mathbb{R}^2$ beschreibt, ist die Lösung des Systems der Schnittpunkt zweier Geraden.

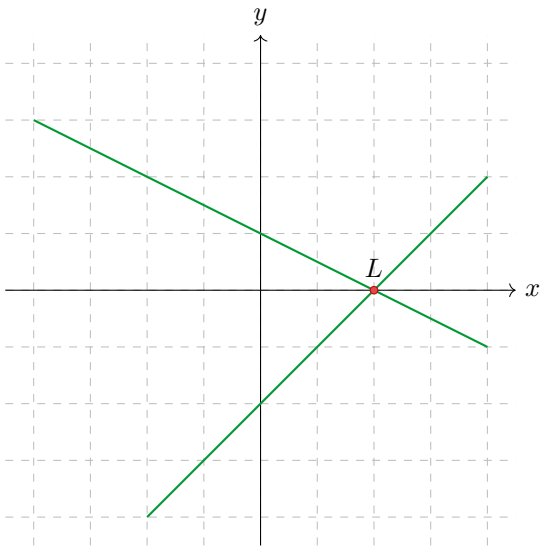

Abbildung 2: Geometrische Darstellung eines linearen Gleichungssystems mit 2 Unbekannten und 2 Gleichungen

Schneiden sich die Geraden in einem Punkt, so existiert genau eine, eindeutige Lösung. Sind die Geraden stattdessen parallel, so existiert keine Lösung, und wenn sie ineinander liegen, so existieren unendlich viele Lösungen.

Wenn wir nun mit 3 Unbekannten und einer Gleichung arbeiten, erhalten wir eine Ebene im $\mathbb{R}^3$, deren Punkte die Gleichung erfüllen:

$$a_1x + a_2y + a_3z = b \Leftrightarrow z = -\frac{a_1}{a_3}x - \frac{a_2}{a_3}y + \frac{b}{a_3}$$

Mit zwei Gleichungen erhalten wir die Schnittgerade zweier Ebenen in $\mathbb{R}^3$. Und zuletzt betrachten wir noch den Fall $m = n = 3$. Dieses System beschreibt den Schnitt von drei Ebenen. Die einzige eindeutige Lösung eines solchen Systems ist ein einzelner Punkt. Weiters kann es möglich sein, dass sich die Ebenen in einer Geraden schneiden, oder sogar ident sind. Sind die Ebenen parallel, so gibt es keine Lösungen, und wenn $a_{ij} = 0$ und $b_i = 0$, so ist $\mathbb{R}^3$ unsere Lösungsmenge.

1.3 Gauß-Elimination

Wir wollen nun ein allgemeines Verfahren betrachten, um lineare Gleichungssysteme zu lösen. Dazu verwenden wir die Gauß-Elimination. Trotz des Namens reicht dieses Verfahren bis ca. 150 n. Chr. in China zurück und tauchte später wieder bei Newton auf. Allerdings stammt die Variante, welche wir heutzutage verwenden. Die Motivation hinter diesem Algorithmus war die Methode der Kleinsten Quadrate, mit der Gauss um 1801 die Laufbahn des Zwergplaneten Ceres korrekt vorhersagte. Später werden wir noch eine erweiterte Version, den Gauß-Jordan-Algorithmus, kennenlernen.

Erarbeiten wir die Funktionsweise anhand eines Beispiels:

$$\begin{aligned} -x + \ \ y + 2z &= 2 \\ 3x - \ \ y + \ \ z &= 6 \\ -x + 3y + 4z &= 4 \end{aligned}$$

Wir beginnen damit, x aus den Gleichungen II und III zu eliminieren, indem wir $II + 3I$ und $III - I$ rechnen. Damit erhalten wir:

$$\begin{aligned} -x + \ \ y + 2z &= \ 2 \\ 0 + 2y + 7z &= 12 \\ 0 + 2y + 2z &= \ 2 \end{aligned}$$

Wir wiederholen den Schritt, und wollen y aus Gleichung III eliminieren und rechnen daher $III - I$:

$$\begin{aligned} -x + \ y + 2z &= \ \ 2 \\ 0 + 2y + 7z &= \ 12 \\ 0 + \ 0 - 5z &= -10 \end{aligned}$$

Aus unserer dritten Zeile erhalten wir nun $z = 2$. Das können wir direkt in die zweite Gleichung einsetzen und erhalten $2y + 14 = 12$ und nach y auflösen. Damit erhalten wir $y = -1$. Zuletzt können wir die Werte von z und y in unsere Gleichung einsetzen und erhalten $-x + (-1) + 2(2) = 2$ und erhalten somit $x = 1$. Wir haben also eine eindeutige Lösung des Gleichungssystems bestimmt.

Die Idee von Gauß war nun, nur noch die Veränderungen der Koeffizienten festzuhalten, indem man die Zeilen der Systemmatrix bearbeitet:

$$\left[\begin{array}{ccc|c} -1 & 1 & 2 & 2 \\ 3 & -1 & 1 & 6 \\ -1 & 3 & 4 & 4 \end{array}\right] \overset{II+3I,\ III-I}{\rightsquigarrow} \left[\begin{array}{ccc|c} -1 & 1 & 2 & 2 \\ 0 & 2 & 7 & 12 \\ 0 & 2 & 2 & 2 \end{array}\right] \overset{III-II}{\rightsquigarrow} \left[\begin{array}{ccc|c} -1 & 1 & 2 & 2 \\ 0 & 2 & 7 & 12 \\ 0 & 0 & -5 & -10 \end{array}\right]$$

Bei dem Algorithmus wählen wir allgemein immer ein **Pivot-Element** und eliminieren dieses Element in allen anderen Gleichungen. Danach wählen wir ein neues Pivot-Element, welches bis jetzt noch keines war, und eliminieren die Unbekannte in allen Gleichungen, in denen noch kein Pivot-Element gewählt wurde. Das wiederholen wir solange, bis wir alle Gleichungen durchgegangen sind, oder wir keine Pivot-Elemente mehr wählen können.

Eine sinnvolle Fortsetzung dieses Rechenschemas ist es, die Elimination "umgekehrt" durchzuführen. Sprich wir wählen unser letztes Pivot-Element und eliminieren es in allen anderen Gleichungen, und wieder holen diesen Schritt, bis wir wieder bei der ersten Gleichung angelangt sind:

$$\left[\begin{array}{ccc|c} -11 & 1 & 2 & 2 \\ 0 & 2 & 7 & 12 \\ 0 & 0 & -5 & -10 \end{array}\right] \overset{-\frac{1}{5}III}{\rightsquigarrow} \left[\begin{array}{ccc|c} -1 & 1 & 2 & 2 \\ 0 & 2 & 7 & 12 \\ 0 & 0 & 1 & 2 \end{array}\right] \overset{II-7III,\ I-2III}{\rightsquigarrow} \left[\begin{array}{ccc|c} -1 & 1 & 0 & -2 \\ 0 & 2 & 0 & -2 \\ 0 & 0 & 1 & 2 \end{array}\right]$$

$$\overset{\frac{1}{2}II,\ -1I}{\rightsquigarrow} \left[\begin{array}{ccc|c} 1 & -1 & 0 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{array}\right] \overset{I+II}{\rightsquigarrow} \left[\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{array}\right]$$

In diesem Fall gibt es eine eindeutige Lösung $(1, -1, 2)$. Betrachten wir ein System, das keine eindeutige Lösung besitzt:

$$\left[\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 1 & -2 & 2 & 2 \\ 4 & 1 & 5 & 5 \end{array}\right] \overset{II-I,\ III-4I}{\rightsquigarrow} \left[\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & -3 & 1 & 1 \\ 0 & -3 & 1 & 1 \end{array}\right] \overset{III-II}{\rightsquigarrow} \left[\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & -3 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

Wir erhalten also eine Nullzeile, womit eine Gleichung überflüssig ist. Wir haben also nur noch zwei Gleichungen, was allerdings nicht ausreicht, um eine eindeutige Lösung zu bestimmen. Wählen wir nun y beliebig in $\mathbb{R}$, so können wir $-3y + z = 1$ nach $z = 1 - 3y$ auflösen. Zuletzt eliminieren wir z in der ersten Gleichung und setzen y ein:

$$x + 4y = 0 \Leftrightarrow x = -4y$$

Wir erhalten also eine Gerade in $\mathbb{R}^3$ als Lösungsmenge:

$$L = \left\{ \begin{bmatrix} -4y \\ y \\ 1 + 3y \end{bmatrix} | y \in \mathbb{R} \right\}$$

Zuletzt betrachten wir ein System, das keine Lösung hat:

$$\left[\begin{array}{ccc|c} 3 & 2 & 1 & 3 \\ 2 & 1 & 1 & 0 \\ 6 & 2 & 4 & 6 \end{array}\right] \overset{II-I,III-4I}{\rightsquigarrow} \left[\begin{array}{ccc|c} 3 & 2 & 1 & 3 \\ 1 & -1 & 0 & -3 \\ -6 & -6 & 0 & -6 \end{array}\right] \overset{III-6II}{\rightsquigarrow} \left[\begin{array}{ccc|c} 3 & 2 & 1 & 3 \\ 2 & -1 & 0 & -3 \\ 0 & 0 & 0 & 12 \end{array}\right]$$

Somit hat dieses Gleichungssystem keine Lösung, da die Gleichung $0 = 12$ für keine $x, y, z \in \mathbb{R}$ erfüllbar ist. Wir können nun den Algorithmus vollständig formulieren:

1. finde $a_{ij} \neq 0$ in einer Zeile, die noch nicht Pivotzeile war, dann heißt a_{ij} Pivotelement, die i-te Zeile Pivotzeile und die j-te Spalte Pivotspalte
2. markiere a_{ij}
3. subtrahiere für alle anderen $k \neq i$ die Pivotzeile multipliziert mit $\frac{a_{kj}}{a_{ij}}$ von den k-ten Zeilen (in der j-ten Spalte entstehen lauter Nullen)
4. wiederhole diese Schritte, bis kein neues Pivotelement zu finden ist, d.h. jede Zeile war bereits eine Pivotzeile, oder es gibt eine Zeile, in der links lauter Nullen sind
5. streiche alle Zeilen, die links und rechts nur Nullen enthalten
6. wenn es eine Zeile gibt, die links nur Nullen enthält, und rechts eine Zahl ungleich 0 enthält, dann gibt es keine Lösung
7. wenn 6. nicht eintritt, erfolgt die Rücksubstitution, bei der wir alle Pivotzeilen in umgekehrter Reihenfolge durch und drücke die Pivotvariablen durch die anderen Variablen aus
8. alle Spalten, die nie zu Pivotspalten wurden, entsprechen freien Parametern
9. die Pivotvariablen lassen sich durch die freien Parameter und die rechte Seite ausdrücken

Ein Gleichungssystem mit 4 Variablen und Gleichungen:

$$\left[\begin{array}{cccc|c} 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 1 & -2 & -3 \\ 2 & 3 & 4 & 5 & 6 \\ 1 & 1 & 1 & 1 & 1 \end{array}\right] \overset{II-I,\ III-2I,\ IV-I}{\rightsquigarrow} \left[\begin{array}{cccc|c} 1 & 2 & 3 & 4 & 5 \\ 0 & -2 & -2 & -6 & -8 \\ 0 & -1 & -2 & -3 & -4 \\ 0 & -1 & -2 & -3 & -4 \end{array}\right]$$

$$\overset{II-2III,\ IV-I}{\rightsquigarrow} \left[\begin{array}{cccc|c} 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & -1 & -2 & -3 & -4 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right] \rightsquigarrow \left[\begin{array}{cccc|c} 1 & 2 & 3 & 4 & 5 \\ 0 & -1 & -2 & -3 & -4 \\ 0 & 0 & 1 & 0 & 0 \end{array}\right]$$

$$\overset{II+2II,\ I-3III}{\rightsquigarrow} \left[\begin{array}{cccc|c} 1 & 2 & 0 & 4 & 5 \\ 0 & -1 & 0 & -3 & -4 \\ 0 & 0 & 1 & 0 & 0 \end{array}\right] \overset{I+2II,-1II}{\rightsquigarrow} \left[\begin{array}{cccc|c} 1 & 0 & 0 & -2 & -3 \\ 0 & 1 & 0 & 3 & 4 \\ 0 & 0 & 1 & 0 & 0 \end{array}\right]$$

Wir erhalten für x_4 einen freien Parameter t. In der dritten Zeile ist $x_3 = 0$ eindeutig bestimmt. Mit der zweiten Zeile bekommen wir $x_2 = 4 - 3t$ und aus der ersten $x_1 = -3 + 2t$. Unsere Lösungsmenge ist daher eine Gerade in $\mathbb{R}^4$:

$$L = \left\{ \begin{bmatrix} -3+2t & 4-3t & 0 & 5 \end{bmatrix} | t \in \mathbb{R} \right\}$$

1.4 Anschauliche Vektorrechnung

Definition 1.1: $\mathbb{R}^n$

Der Raum $\mathbb{R}^n$ ist die folgende Menge:

$$\mathbb{R}^n = \left\{ \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} | a_i \in \mathbb{R} \colon i = 1, 2, \ldots, n \right\}$$

Es handelt sich hierbei um die Menge (Raum) der n-dimensionalen Spaltenvektoren. Wir können eine Addition definieren:

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} + \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} a_1 + b_1 \\ a_1 + b_2 \\ \vdots \\ a_n + b_n \end{bmatrix}$$

Die Multiplikation mit einer reellen Zahl λ:

$$\lambda \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} \lambda a_1 \\ \lambda a_2 \\ \vdots \\ \lambda a_n \end{bmatrix}$$

Zusätzlich benötigen wir die Subtraktion:

$$- \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} -a_1 \\ -a_2 \\ \vdots \\ -a_n \end{bmatrix}$$

Und einen Nullvektor:

$$0 = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Der Nullvektor hat die Eigenschaft $\boldsymbol{a} + 0 = \boldsymbol{a}$ für alle $\boldsymbol{a} \in \mathbb{R}^n$.

Wir können den $\mathbb{R}^n$ für $n = 1, 2, 3$ geometrisch deuten. Hierbei entspricht die Addition einer **Translation** und die Multiplikation einer Verlängerung bzw. einer Verkürzung eines Vektors. Wir stellen Vektoren dabei als Pfeile bzw. Translationen darstellen. Ein Vektor $\boldsymbol{a} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$ kann beliebig in der Ebene als Pfeil dargestellt werden, allerdings sind alle Darstellungen der selbe Vektor.

Bemerkung 1.2

Haben zwei Pfeile die gleiche Länge und Richtung, so werden sie als ein Vektor identifiziert.

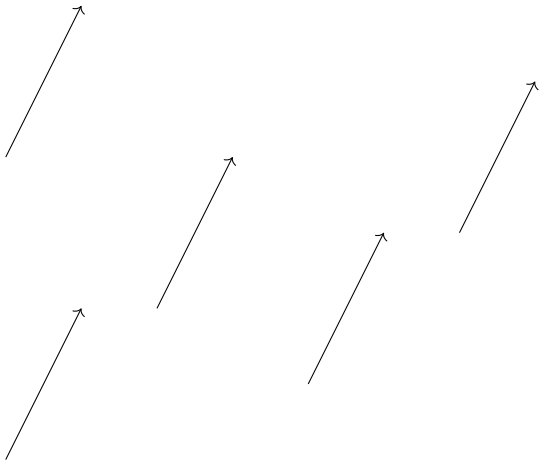

Abbildung 3: Einige identische Vektoren

Bemerkung 1.3

Wenn man einen Nullpunkt festlegt, dann ist jeder Punkt um Raum eindeutig durch seinen Ortsvektor festgelegt. Jeder Vektor entspricht auch einem Punkt im Raum.

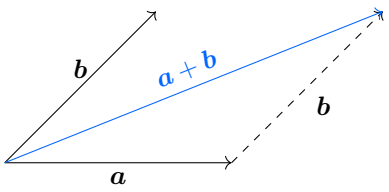

Abbildung 4: Graphische Darstellung der Vektoraddition als Parallelverschiebung

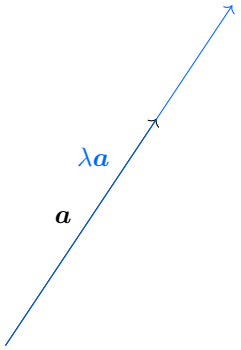

Abbildung 5: Graphische Veranschaulichung der Skalarmultiplikation eines Vektors

Wir betrachten einige Eigenschaften der Vektoraddition. Seien $\boldsymbol{a}$, $\boldsymbol{b}$ und $\boldsymbol{c}$ Vektoren in $\mathbb{R}^n$, so gelten die folgenden Gesetze:

- Kommutativgesetz $\boldsymbol{a} + \boldsymbol{b} = \boldsymbol{b} + \boldsymbol{a}$ ($a_i + b_i = b_i + a_i$ gilt koordinatenweise)
- Assoziativgesetz $(\boldsymbol{a} + \boldsymbol{b}) + \boldsymbol{c} = \boldsymbol{a} + (\boldsymbol{b} + \boldsymbol{c})$ (gilt koordinatenweise)

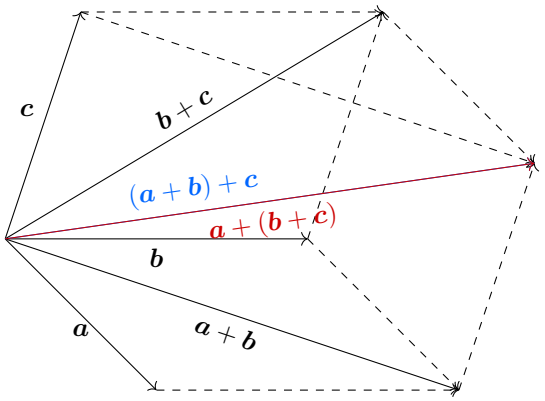

Abbildung 6: Graphische Darstellung des Assoziativgesetzes der Vektoraddition

Wir können das Assoziativgesetz einfach auf die Assoziativität der reellen Zahlen zurückführen:

$$\boldsymbol{a} + (\boldsymbol{b} + \boldsymbol{c}) = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} + \begin{bmatrix} b_1 + c_1 \\ b_2 + c_2 \\ \vdots \\ b_n + c_n \end{bmatrix} = \begin{bmatrix} a_1 + (b_1 + c_1) \\ a_2 + (b_2 + c_2) \\ \vdots \\ a_n + (b_n + c_n) \end{bmatrix} = \begin{bmatrix} (a_1 + b_1) + c_1 \\ (a_2 + b_2) + c_2 \\ \vdots \\ (a_n + b_n) + c_n \end{bmatrix} = (\boldsymbol{a} + \boldsymbol{b}) + \boldsymbol{c}$$

Auch bei der Skalarmultiplikation gelten einige Gesetze:

- Assoziativgesetz $\lambda(\mu\boldsymbol{a}) = (\lambda\mu)\boldsymbol{a}$
- Distributivgesetz 1 $(\lambda + \mu)\boldsymbol{a} = \lambda\boldsymbol{a} + \mu\boldsymbol{a}$
- Distributivgesetz 2 $\lambda(\boldsymbol{a} + \boldsymbol{b}) = \lambda\boldsymbol{a} + \lambda\boldsymbol{b}$

Betrachten wir ein konkretes Beispiel der anschaulichen Vektorrechnung. Wir wollen zeigen, dass sich die Diagonalen eines Parallelogramms einander halbieren:

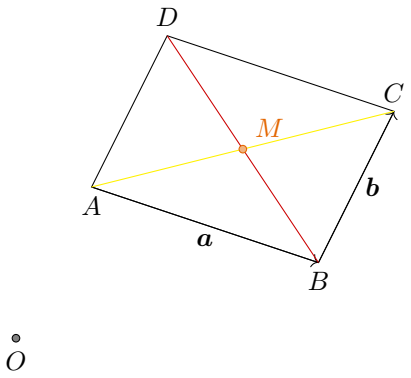

Abbildung 7: Ein Parallelogramm mit seinen Diagonalen

Wir behaupten nun, dass M, der Mittelpunkt der Strecke $\overrightarrow{AC}$, und N, der Mittelpunkt der Strecke $\overrightarrow{BD}$ gleich sind. Dazu stellen wir die Ortsvektoren auf:

$$\overrightarrow{OM} = \overrightarrow{OA} + \frac{1}{2}\overrightarrow{AC} = \overrightarrow{OA} + \frac{1}{2}\left(\overrightarrow{AB} + \overrightarrow{BC}\right) = \overrightarrow{OA} + \frac{1}{2}(\boldsymbol{a} + \boldsymbol{b})$$

$$\overrightarrow{ON} = \overrightarrow{OB} + \frac{1}{2}\overrightarrow{BD} = \overrightarrow{OB} + \frac{1}{2}\left(\overrightarrow{BC} + \overrightarrow{CD}\right) = \overrightarrow{OB} + \frac{1}{2}(\boldsymbol{b} - \boldsymbol{a})$$

$$= \overrightarrow{OA} + \overrightarrow{AB} + \frac{1}{2}(\boldsymbol{b} - \boldsymbol{a}) = \overrightarrow{OA} + \boldsymbol{a} + \frac{1}{2}(\boldsymbol{b} + \boldsymbol{a}) = \overrightarrow{OA} + \frac{1}{2}(\boldsymbol{b} + \boldsymbol{a}) = \overrightarrow{OM}$$

2 Algebraische Strukturen

Definition 2.1: Algebraische Struktur

Eine algebraische Struktur ist eine Menge M mit einer Verknüpfung $\circ$, (z.B. $+$ oder $\cdot$), sodass für alle $a, b \in M$: $c = a \circ b \in M$ gilt.

Die Verknüpfung einer algebraischen Struktur ist eine Funktion der Form $\circ : M \times M \to M$ mit $(a, b) \mapsto a \circ b$. Dabei kann $a \circ b$ auf verschiedene Arten festgelegt werden. Allgemein bezeichnen wir eine algebraische Struktur mit $(M, \circ)$. Ein besonders einfaches Beispiel sind etwa die reellen Zahlen mit der üblichen Multiplikation:

$$(\mathbb{R}, +) \quad a, b \in \mathbb{R} \Rightarrow a + b \in \mathbb{R}$$

Die Verknüpfung $+$ ist in den reellen Zahlen also abgeschlossen. Auch die Multiplikation in $(\mathbb{R}, \cdot)$, oder $(\mathbb{N}, \cdot)$ ist abgeschlossen. Ein klassisches Beispiel einer nicht algebraischen Struktur ist $(\mathbb{N}, -)$, da nicht für alle $a, b \in \mathbb{N}$ garantiert ist, dass $a - b$ in $\mathbb{N}$ liegt. Anders verhält sich das in $\mathbb{R}$, da hier negative Zahlen enthalten sind.

Die Grundrechenarten liefern oftmals ohne viel Nachdenken bzw. ohne große Ausnahmen, algebraische Strukturen auf den gängigen Zahlenmengen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$. Allerdings können wir auch Funktion wir z.B. auch $(\mathbb{R}, \max)$ betrachten. Das Maximum liegt offensichtlich immer in den reellen Zahlen. Betrachten wir $M = \{\pm 1\}$ und $a \circ b = a \cdot b$. Da die Menge M endlich ist, können wir alle möglichen Kombinationen in einer **Verknüpfungstabelle** aufstellen:

$\circ$	$+1$	-1
$+1$	$+1$	-1
-1	-1	$+1$

Tabelle 2: Verknüpfungstabelle der Struktur $(\{\pm 1\}, \cdot)$

Auch der Durchschnitt zweier Mengen A und B aus der Struktur $(\mathcal{P}(X), \cap)$ mit einer beliebigen Menge X ist eine algebraische Struktur, da der Durchschnitt zweier Mengen höchstens leer sein kann. Der Durchschnitt ist also abgeschlossen, da die leere Menge ein Element der Potenzmenge von X ist.

Eine weiter Möglichkeit, eine Verknüpfung zu definieren, ist, die Verknüpfungstabelle festzulegen. Dabei legen wir die Ergebnisse der Verknüpfungen einzeln fest. Betrachten wir etwa $M = \{a, b, c, e\}$:

$\circ$	a	b	c	e
a	e	c	b	a
b	c	e	a	b
c	b	a	e	c
e	a	b	c	e

Tabelle 3: Definition einer Verknüpfung mittels Verknüpfungstabelle

Eine etwas interessantere Verknüpfung ist die **Konkatenation**. Hierbei arbeiten wir mit einem Alphabet aus Symbolen $A = \{a, b, c, \dots\}$ und bestimmen über unseren Alphabet Wörter als Folge von Symbolen in A, welche wir in einer Menge M festhalten. Die Konkatenation ist nun eine Verknüpfung, welche Wörter aneinanderhängt:

$$a_1 \dots a_m \circ b_1 \dots b_n = a_1 \dots a_m b_1 \dots b_n \in M$$

Das neue Wort $a \circ b$ hat die Länge $m + n$. Diese Operation ist offensichtlich nicht kommutativ.

Definition 2.2: Assoziativität, neutrales Element und inverses Element

Sei $(M, \circ)$ eine algebraische Struktur:

i) Die Verknüpfung $\circ$ heißt **assoziativ**, wenn für alle $x, y, z \in M$ $(x \circ y) \circ z = x \circ (y \circ z)$ gilt

ii) Ein Element $e \in M$ heißt linksneutral, wenn $\forall x \in M : e \circ x =$ und rechtsneutral, wenn $\forall x \in M : x \circ e = x$. Wir bezeichnen e als neutrales Element, wenn $e \circ x = x = x \circ e$ gilt.
iii) Wenn ein neutrales Element existiert, dann heißt y linksinvers zu x, wenn $y \circ x = e$, und rechtsinvers, wenn $x \circ y = e$ gilt. Wir bezeichnen y als inverses Element, wenn $y \circ x = e = x \circ y$ gilt.

Definition 2.3: Halbgruppe, Monoid und Gruppe

Eine assoziative algebraische Struktur $(M, \circ)$ heißt **Halbgruppe**. Existiert in M ein neutrales Element bezüglich $\circ$, so bezeichnet man $(M, \circ)$ als **Monoid**. Ist jedes Element in M eines Monoiden invertierbar, so bezeichnet man $(M, \circ)$ als **Gruppe**.
Ist die Verknüpfung $\circ$ kommutativ auf M, so nennen wir die Algebraische Struktur $(M, \circ)$ **abelsch**.

Die Bezeichnung abelsch stammt von dem norwegischen Mathematiker Nils Henrik ABEL, einem der Urväter der Gruppentheorie. Betrachten wir wieder einige der algebraischen Strukturen, welche wir zuvor erörtert haben:

$(\mathbb{R}, +)$	abelsche Gruppe	$(\mathbb{N}, \cdot)$	abelsches Monoid
$(\mathbb{R}, \cdot)$	abelsches Monoid	$(\mathbb{N}, +)$	abelsche Halbgruppe
$(\mathbb{R} \setminus \{0\}, \cdot)$	abelsche Gruppe	$(\mathbb{N}_0, +)$	abelsches Monoid
$(\mathbb{R} \setminus \{0\}, +)$	keine algebraische Struktur	$(\mathbb{N}, \circ)$ mit $a \circ b = a^b$	nicht assoziativ

Tabelle 4: Einige Beispiele von (algebraischen) Strukturen

Satz 2.1: Abschwächung der Gruppenaxiome

Sei M eine Menge und $\circ$ eine Verknüpfung, so ist $(M, \circ)$ eine Gruppe, wenn gilt:

$$\forall x, y, z \in G \colon (x \circ y) \circ z = x \circ (y \circ z) \tag{G1}$$
$$\exists e \in M \colon \forall x \in M \colon e \circ x = x \tag{G2}$$
$$\forall x \in M \colon \exists y \in M \colon y \circ x = e \tag{G3}$$

Beweis. Zu zeigen ist, dass $\forall x \in M \colon x \circ e = x$ und $\forall x \in M \colon \exists y \in M \colon x \circ y = e$ erfüllt sind, indem wir nur (G1), (G2) und (G3) verwenden.

Sei $x \in M$, aus (G3) folgt $\exists y \colon y \circ x = e$. Weiters folgt aus (G3) $\exists z \colon z \circ y = e$.

$$x \circ y \overset{(G2)}{=} e \circ (x \circ y) = (z \circ y) \circ (x \circ y)$$
$$\overset{(G1)}{=} z \circ ((y \circ x) \circ y) \overset{(G3)}{=} z \circ (e \circ y) \overset{(G2)}{=} z \circ y = e$$

Wir haben somit gezeigt, dass auch $x \circ y = e$ erfüllt ist.

Sei $x \in M$ und $y \in M$, sodass $y \circ x = e$ (G2).

$$x \circ e = x \circ (y \circ x) \overset{(G1)}{=} (x \circ y) \circ x = e \circ x \overset{(G2)}{=} x$$

□

Satz 2.2: Eindeutigkeit von neutralem Element und inversen Element

Sei $(G, \circ)$ eine Gruppe, dann sind das neutrale Element und das inverse Element eindeutig. Zusätzlich

gibt es Kürzungsregeln der Form:

$$\forall x, y, z \colon x \circ y = x \circ z \Rightarrow y = z$$
$$\forall x, y, z \colon x \circ z = y \circ z \Rightarrow x = y$$

Beweis. Angenommen e' ist ein weiteres neutrales Element: (1): $\forall x \in G \colon x \circ e' = x$ wobei (2): $\forall x \in G \colon e \circ x = x$ bestehen bleibt:

$$e' \overset{(1)}{=} e \circ e' \overset{(2)}{=} e$$

Seien y, y' zwei inverse Elemente zu $x \in G$. Es gilt also (1): $y \circ x = x \circ y = e$ und (2): $y' \circ x = x \circ y' = e$.

$$y = y \circ e = y \circ (x \circ y') = (y \circ x) \circ y' = e \circ y' = y'$$

Sei u das inverse Element zu $x \in G$, d.h. $u \circ x = e$:

$$\begin{aligned} & u \circ (x \circ y) = u \circ (x \circ z) \\ \Leftrightarrow\ & (u \circ x) \circ y = (u \circ x) \circ z \\ \Leftrightarrow\ & e \circ y = e \circ z \Leftrightarrow y = z \end{aligned}$$

Sei u das inverse Element zu $z \in G$:

$$\begin{aligned} & (x \circ z) \circ u = (y \circ z) \circ u \\ \Leftrightarrow\ & x \circ (z \circ u) = y \circ (z \circ u) \\ \Leftrightarrow\ & x \circ e = y \circ e \\ \Leftrightarrow\ & x = y \end{aligned}$$

□

Definition 2.4: Schreibweise

Das nach Satz 2 eindeutige inverse Element zu x wird mit x^{-1} bezeichnet. Allgemein schreiben wir:

$$x^n = \begin{cases} \underbrace{x \circ x \circ \cdots \circ x}_{n \text{ mal}} & n > 0 \\ \underbrace{x^{-1} \circ x^{-1} \circ \cdots \circ x^{-1}}_{n \text{ mal}} & n < 0 \\ e & n = 0 \end{cases}$$

Dann gilt $\forall m, n \in \mathbb{Z} \colon x^m \circ x^n = x^{m+n}$.
Abelsche Gruppen werden für gewöhnlich additiv geschrieben, also $(G, +)$.

$$\begin{aligned} & x^{-2} \circ x^3 = (x^{-1} \circ x^{-1}) \circ (x \circ x \circ x) \\ & = x^{-1} \circ x^{-1} \circ x \circ x \circ x = x^{-1} \circ e \circ x \circ x \\ & = x^{-1} \circ x \circ x = e \circ x = x = x^{-2+3} \end{aligned}$$

Satz 2.3

Sei $(M, \circ)$ ein Monoid, dann ist die mit der Menge $G = \{x \in M \colon \exists x^{-1} \in M \colon x \circ x^{-1} = e\}$ festgelegte Struktur $(G, \circ)$ eine Gruppe.

Beweis. Wir müssen also zeigen, dass für $(G, \circ)$ die drei Gruppenaxiome erfüllt sind. Zu zeigen sind also:

$$\begin{aligned} &1) \quad \forall x, y \in G \colon x \circ y \in G \\ &2) \quad \exists e \in G \colon x \circ e = x \\ &3) \quad x \in G \Rightarrow x^{-1} \in G \end{aligned}$$

Es ist nicht nötig nachzuweisen, dass $\circ$ assoziativ ist, da das bereits von $(M, \circ)$ geerbt wird. Beginnen wir mit 1). Seien $x, y \in G$, so muss $x \circ y \in G$ gelten, sprich $x \circ y$ ist invertierbar. Gesucht ist also ein $z \in G$, sodass $(x \circ y) \circ z = e$. Seien x^{-1} und y^{-1} die Inversen von x und y:

$$\begin{aligned} (x \circ y) \circ \underbrace{(y^{-1} \circ x^{-1})}_{=z} &= x \circ (y \circ y^{-1}) \circ x \\ = x \circ e \circ x^{-1} &= x \circ x^{-1} = e \end{aligned}$$

Unser z ist also $y^{-1} \circ x^{-1}$, damit ist $(x \circ y)$ invertierbar, womit $(G, \circ)$ eine Halbgruppe ist. Weiters müssen wir 2) zeigen:

$$e \circ e = e \Rightarrow e = e^{-1} \in G$$

Zuletzt 3): $\exists z \in G \colon x^{-1} \circ z = e$. Wir kennen so ein z, nämlich x: $x^{-1} \circ x = e$. □

2.1 Gruppen und Funktionen

Wir wollen nun eine der wichtigsten Gruppen erarbeiten. Dazu betrachten wir zuerst eine Menge X mit $X^X = \{\varphi : X \to X\}$, also die Menge aller Funktionen von X nach X. Für $f, g \in X^X$ ist $f \circ g(x) := f(g(x))$. Die verknüpfte Funktion $f \circ g$ liegt wieder in X^X und diese Verknüpfung ist assoziativ:

$$\begin{aligned} &f, g, h \in X^X \\ &(f \circ g) \circ h = f(g(x)) \circ h = f(g(h(x))) = f \circ g(h(x)) = f \circ (g \circ h) \end{aligned}$$

Wir haben also mit $(X^X, \circ)$ eine Halbgruppe. Weiters suchen wir ein neutrales Element $e \colon X \to X$, sodass $\forall f \in X^X \colon f \circ e = f$. Wir sagen dazu, dass zwei Funktionen $f, g \in X^X$ gleich sind, wenn $\forall x \in X \colon f(x) = g(x)$ gilt. Damit muss also $\forall x \in X \colon f(e(x)) = f(x)$ gelten. Sei $\mathrm{id} : X \to X$ mit $x \mapsto x$, Damit $f(e(x)) = f(x)$ erfüllt ist, muss $e(x) = x$ gelten. Unser neutrales Element e ist also id. Die Struktur $(X^X, \circ)$ ist also ein Monoid mit dem neutralen Element id.

Wie zuvor, damit $(X^X, \circ)$ eine Gruppe ist, bestimmen wir einfach alle invertierbaren Elemente $f \in X^X$. Erarbeiten wir die invertierbaren Funktionen anhand des Beispiels $X = \{1, 2\}$. Wir können die folgenden Funktionen auf X definieren:

Funktion	$f(1)$	$f(2)$
f_{12}	$1 \mapsto 1$	$2 \mapsto 2$
f_{11}	$1 \mapsto 1$	$2 \mapsto 1$
f_{22}	$1 \mapsto 2$	$2 \mapsto 2$
f_{21}	$1 \mapsto 2$	$2 \mapsto 1$

Tabelle 5: Alle Funktionen auf $X = \{1, 2\}$

$\circ$	f_{12}	f_{11}	f_{22}	f_{21}
f_{12}	f_{12}	f_{11}	f_{22}	f_{21}
f_{11}	f_{11}	f_{11}	f_{11}	f_{11}
f_{22}	f_{22}	f_{22}	f_{22}	f_{22}
f_{21}	f_{21}	f_{22}	f_{11}	f_{12}

Tabelle 6: Verknüpfungstabelle von $(X^X, \circ)$ mit $X = \{1, 2\}$

Wir sehen, dass nur f_{12} und f_{21} invertierbar sind. Wir bezeichnen $(\{f_{12}, f_{21}\}, \circ)$ als die symmetrische Gruppe mit zwei Elementen, S_2.

Definition 2.5: Permutationsgruppe

Sei $X = \{x_1, x_x \dots, x_n\}, n \in \mathbb{N}$ eine Menge, so bezeichnen wir $(S_X, \circ)$ mit $S_X = \{f \colon X \to X | \exists f^{-1} \in X^X : f \circ f^{-1} = \mathrm{id}\}$ als die Gruppe aller Permutationen der Elemente in X. Es gilt dann $|S_X| = n!$.
Wir schreiben dann (z.B. für S_3):

$$f_{213} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad f_{123} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \dots$$

Die Symmetriegruppen können sehr gut anhand von Transformationen regelmäßiger Figuren (Dreiecke, Quadrate, usw.) in der Ebene dargestellt werden. Betrachten wir jedoch ein Rechteck mit ungleichen Seiten, gibt es weniger Transformationen, welche das Rechteck in sich überführen.

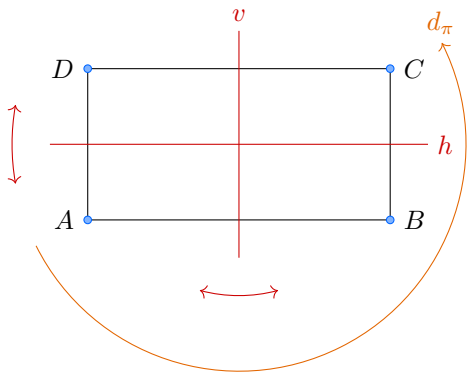

Abbildung 8: Erhaltende Transformationen eines ebenen Rechtecks

Die Transformation h spiegelt das Rechteck horizontal und bildet (A, B, C, D) auf (D, C, B, A) ab. Analog spiegelt v das Rechteck vertikal und bilde (A, B, C, D) auf (B, A, D, C) ab. Zusätzlich können wir mit d_π um 180° drehen, dabei wird (A, B, C, D) auf (B, C, D, A) abgebildet. Zuletzt gibt es die Transformation id, bei der wir keine Transformation anwenden und (A, B, C, D) auf (A, B, C, D) abbilden.

2.1.1 Funktionen

Definition 2.6: Funktionen

Seien X, Y Mengen, so nennen wir die Funktion $f : X \to Y$ (auch Abbildung), eine Vorschrift, mit welcher wir einen Wert $x \in X$ auf einen Wert (ein Bild) $y \in Y$ abbilden (wir ordnen einem x ein y zu).

Ein klassisches Beispiel ist das Quadrat der reellen Zahlen $f : \mathbb{R} \to [0, \infty)$ mit $x \mapsto x^2$.

Definition 2.7: Injektivität, Surjektivität, Bijektivität

Sei $f : X \to Y$ eine Funktion mit $x \mapsto f(x)$. Wir nennen f injektiv, wenn gilt:

$$\forall x_1, x_2 \in X \colon x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

Weiters nennen wir f surjektiv, wenn gilt:

$$\forall y \in Y \colon \exists x \in X \colon f(x) = y$$

Eine Funktion f ist bijektiv, wenn sie injektiv und surjektiv ist. Wenn f bijektiv ist, existiert die Umkehrfunktion f^{-1}.

2.1.2 Kongruenzen

Definition 2.8: Rechnen modulo n

Sei $n \in \mathbb{N}$ und $n \geq 2$, $x, y \in \mathbb{Z}$. Wir sagen $x \equiv y \mod n$ (x kongruent zu y modulo n), wenn gilt: $y - x$ ist ein ganzzahliges Vielfaches von n, d.h. $n|y - x$. Das heißt $\exists k \in \mathbb{N}$: $y - x = kn$.
Die Kongruenzklasse (auch Restklasse) von $x \in \mathbb{Z} \mod n$ ist die Menge $[x]_n = \{y \in \mathbb{Z} : x \equiv y \mod n\}$.

Sei $n \in \mathbb{N}$, dann nennen wir $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$ mit $|\mathbb{Z}_n| = n$. Jede Zahl $x \in \mathbb{Z}$ kann geschrieben werden als $x = kn + r$ wobei $k \in \mathbb{Z}$ und $r \in \{0, \ldots, n-1\}$. Wir wissen bereits, dass wir für positive $k \in \mathbb{Z}$ einen positive Rest r finden können. Wir wollen auch für negative $k \in \mathbb{Z}$ einen positiven Rest finden. Für 7 in $\mathbb{Z}_3$ wäre das etwa 2, da $-3 \cdot 3 + 2 = -7$, womit $-7 \in [2]_3$. Somit liegt jede Zahl in $\mathbb{Z}$ in einer Restklasse $[r]_n$ mit $r \in \{0, \ldots, n-1\}$. Somit gilt $\mathbb{Z} = [0]_n \cup [1]_n \cup \cdots \cup [n-1]_n$. Weiters sind die Restklassen von $\mathbb{Z}_n$ alle disjunkt, da eine Zahl $k \in \mathbb{Z}$ nur einen Rest hat. Somit, wenn $k \neq l$, dann $[k]_n \cap [l]_n = \emptyset$. Auf $\mathbb{Z}_n$ definieren wir $[x]_n + [y]_n = [x + y]_n$ und $[x]_n \cdot [y]_n = [x \cdot y]_n$. Dürfen wir uns diese Operationen einfacht so zurechtlegen?.

Satz 2.4: Rechenoperationen auf $\mathbb{Z}_n$

(i) Die Addition auf $\mathbb{Z}_n$ ist wohldefiniert. Wenn $x_1 \equiv x_2 \mod n$ und $y_1 \equiv y_2 \mod n$, dann ist auch $x_1 + y_1 \equiv x_2 + y_2 \mod n$. Das heißt, wenn $[x_1]_n = [x_2]n$ und $[y_1]_n = [y_2]_n$, dann ist auch $[x_1 + y_2]_n = [x_2 + y_2]_n$. Und $(\mathbb{Z}_n, +)$ ist eine abelsche Gruppe mit dem neutralen Element $[0]_n$.
(ii) Die Multiplikation auf $\mathbb{Z}_n$ ist wohldefiniert. Wenn $x_1 \equiv x_2 \mod n$ und $y_1 \equiv y_2 \mod n$, dann dann ist auch $x_1 \cdot y_1 \equiv x_2 \cdot y_2 \mod n$. Und $(\mathbb{Z}_n, \cdot)$ ist ein abelsches Monoid mit neutralem Elemente $[1]_n$.

Beweis. Sei $x_1 \equiv x_2 \mod n$ und $y_1 \equiv y_2 \mod n$, sprich $[x_1]_n = [x_2]_n$ und $[y_1]_n = [y_2]_n$. Zu zeigen ist $x_1 + y_1 \equiv x_2 + y_2 \mod n$ und $x_1 \cdot y_1 \mod x_2 \cdot y_2 \mod n$. Wir wissen $\exists k \in \mathbb{Z}$: $x_2 = x_1 + kn$ und $\exists l \in \mathbb{Z}$: $y_2 = y_1 + ln$:

$$x_2 + y_2 = y_1 + kn + y_1 ln = (x_1 + y_1) + (k + l)n \Rightarrow x_2 + y_2 \equiv x_1 + y_1 \mod n$$
$$x_2 y_2 = (x_1 + kn)(y_1 + ln) = x_1 y_1 + kny_1 + x_1 ln + knln = x_1 y_1 + (ky_1 + lx_1 + kln)n \Rightarrow x_2 y_2 \equiv x_1 y_1 \mod n$$

(i) Wir müssen noch zeigen, dass $(\mathbb{Z}_n, +)$ eine abelsche Gruppe ist. Dabei ist die Abgeschlossenheit bereits erfüllt. Weiter mit der Assoziativität. Seien $[x]_n, [y]_n, [z]_n \in \mathbb{Z}_n$:

$$[x]_n + ([y]_n + [z]_n) = [x]_n + [y + z]_n = [x + (y + z)]_n = [(x + y) + z]_n = [x + y]_n + [z]_n = ([x]_n + [y]_n) + [z]_n$$

Die Kommutativität erfolgt analog:

$$[x]_n + [y]_n = [x + y]_n = [y + x]_n = [y]_n + [x]_n$$

Das neutrale Elemente ist $[0]_n$:

$$[x]_n + [0]_n = [x + 0]_n = [x]_n$$

Wir brauhen nur noch ein inverses Element, also $\forall [x]_n \in \mathbb{Z}_n : \exists [y]_n \in \mathbb{Z}_n : [x]_n + [y]_n = [0]_n$. In $\mathbb{Z}$ wählen wir $y = -x$. In $\mathbb{Z}_n$ ginge das auch, eleganter ist aber $y = n - x$:

$$[x]_n + [n - x]_n = [x + n - x]_n = [n]_n = [0]_n$$

(ii) Wir prüfen noch, ob $(\mathbb{Z}_n, \cdot)$ ein Monoid ist. Die Abgeschlossenheit der Multiplikation ist dabei bereits erfüllt. Seien $[x]_n, [y]_n, [z]_n \in \mathbb{Z}_n$:

$$[x]_n \cdot ([y]_n \cdot [z]_n) = [x]_n \cdot [y \cdot z]_n = [x \cdot (y \cdot z)]_n = [(x \cdot y) \cdot z]_n = [x \cdot y]_n \cdot [z]_n = ([x]_n \cdot [y]_n) \cdot [z]_n$$

Die Kommutativität erfolgt analog:

$$[x]_n \cdot [y]_n = [x \cdot y]_n = [y \cdot x]_n = [y]_n \cdot [x]_n$$

Weiters brauchen wir ein neutrales Element $[1]_n$:

$$[x]_n \cdot [1]_n = [x \cdot 1]_n = [x]_n$$

□

Damit $\mathbb{Z}_n$ eine Gruppe ist, müssen wir die $[0]_n$ entfernen, da $\forall x \in \mathbb{Z}_n : x \cdot 0 = 0$. Wir bezeichnen $(\mathbb{Z}_n^*, \cdot)$ als Gruppe. Für $\mathbb{Z}_2$ gilt $\mathbb{Z}_2^* = \{[1]_2\}$, was eine triviale Gruppe ergibt. Für $\mathbb{Z}_3$ ist $\mathbb{Z}_3^* = \{[1]_3, [2]_3]\}$ bildet mit $\cdot$ eine Gruppe. Für $\mathbb{Z}_4$ ist $\mathbb{Z}_4^* = \{[0]_4, [2]_4\}$. Da 5 ei ne Primzahl ist, gilt $\mathbb{Z}_5^* = \mathbb{Z}_5 \setminus \{[0]_5\}$. Für $\mathbb{Z}_6$ ist $\mathbb{Z}_6^* = \{[1]_6, [5]_6\}$.

Allgemein schrieben wir $G_n = \{[k]_n : \text{ggT}(k, n) = 1\}$.

2.1.3 Morphismen

Wenn wir die Verknüpfungstabellen für $(\{+1, -1\}, \cdot)$, $(\mathbb{Z}_2, +)$ und $(S_2, \circ)$ betrachten, so sehen wir, dass alle drei Tabellen die selbe Strukture haben. Da die Elemente der Gruppen jedoch nicht gleich sind, wollen wir auch nicht sagen, dass die Gruppen gleich sind.

Definition 2.9: Homomorphismus

Sieen $(G_1, \circ_1)$ und $(G_2, \circ_2)$ Gruppen. Eine Abbildung $h : G_1 \to G_2$ heißt (Gruppen)-Homomorphismus, wenn gilt $\forall x, y \in G_1 : h(x \circ_1 y) = h(x) \circ_2 h(y)$.

Ein trivialer Homomorphismus ist $h : G_1 \to G_2$ mit $\forall x \in G_1 : x \mapsto e_2$, wobei e_2 das neutrale Element von G_2 ist. Hier ist die Bedingung für einen Homomorphismus immer erfüllt.

Ein injektiver Homomorphismus h heißt Einbettung. Ein surjektiver Homomorphismus heißt Epimorphismus, und ein bijektiver Homomorphismus ist ein Isomorphismus. Zwei Gruppen G_1 und G_2 heißen isomporph, $G_1 \simeq G_2$, wenn es einen Isomorphismus $h : G_1 \to G_2$. Jede Gruppe $G \simeq G$ mit $h = \text{id}$ für $\text{id} : G \to G$ und $x \mapsto x$. Ein solcher Isomorphismus von $G \to G$ heißt Automorphismus. Ein Homomorphismus $h : G \to G$ heißt Endomorphismus.

Beispiel: $(\mathbb{Z}, +)$ ist eine Gruppe. Sei $h_n : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ mit $x \mapsto nx$:

$$h_n(x + y) = n(x + y) = nx + ny = h_n(x) + h_n(y)$$

Somit ist h_n ein Endomorphismus. Für $n = 1$ ist h_n die identische Abbildung. Für $n \geq 2$ ist h_n nicht surjektiv. Allerdigns ist h_n injektiv, da $nx = ny \Leftrightarrow x = y$.

Beispiel: $q_n : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ mit $x \mapsto [x]_n]$:

$$q_n(x + y) = [x + y]_n = [x]_n + [y]_n = q_n(x) + q_n(y)$$

Somit ist q_n ein Homomorphismus. q_n ist nicht injektiv, da $[0]_n = [n]_n$, sprich $q_n(0) = q_n(n)$. Aber q_n ist surjektiv, da $[k]_n = q_n(k)$ mit $k \in \{0, 1 \ldots, n - 1\}$. Somit ist q_n ein Epimorphismus.

Beispiel: $h : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ mit $x \mapsto -x$:

$$h(x + y) = -(x + y) = -x - y = -y + (-y) = h(x) + h(y)$$

Somit ist h ein Homomorphismus. Zusatzälich ist h bijektiv, weil $x \neq y \Rightarrow -x \neq -y$ und $y = -(-y) = h(-y)$. Somit ist h ein Isomorphismus bzw. ein Automorphismus und nicht die identische Abbildung.

Beispiel: $h_\alpha : (\mathbb{Z}, +) \to (\mathbb{R}^*, \cdot)$ mit $k \mapsto \alpha^k$:

$$h_\alpha(k + l) = \alpha^{k+l} = \alpha^k \alpha^l = h_\alpha(k) h_\alpha(l)$$

h_α ist injektiv, wenn $\alpha \notin \{-1, 1\}$, aber nicht surjektiv.

Beispiel: $\sigma : (\mathbb{R}^+ \cdot) \to (\{\pm 1\}, \cdot)$ mit $x \mapsto \text{sign}(x)$, wobei:

$$\text{sign}(x) = \begin{cases} 1 & x > 0 \\ -1 & x < 0 \end{cases}$$

σ ist ein Homomorphismus:

$$\begin{aligned} &\sigma(xy) = \sigma(x)\sigma(y) \\ &x > 0 \wedge y > 0 \Rightarrow xy > 0 \\ &x < 0 \wedge y < 0 \Rightarrow xy > 0 \\ &x > 0 \wedge y < 0 \Rightarrow xy < 0 \\ &x < 0 \wedge y > 0 \Rightarrow xy < 0 \end{aligned}$$

Beispiel: $h\colon (\mathbb{R},+) \to (\mathbb{R}_+,\cdot)$ mit $x \mapsto \mathrm{e}^x$ ist ein Isomorphismus mit der Umnkehrfunktion $\ln\colon (\mathbb{R}_+,\cdot) \to (\mathbb{R},+)$ und $x \mapsto \ln(x)$.

Satz 2.5

(i) Wenn $h_1\colon G_1 \to G_2$ und $h_2\colon G_2 \to G_3$ Homomorphismen sind, dann ist $h_2 \circ h_1\colon G_1 \to G_2$ auch ein Homomorphismus.
(ii) Wenn $h\colon G_1 \to G_2$ ein Isomorphismus ist, dann ist $h^{-1} : G_2 \to G_1$ auch ein Isomorphismus.
(iii) Die Automorphismen einer Gruppe bilden eine Gruppe.

Beweis. (i) Zu zeigen ist $(h_2 \circ h_1)(x \circ_1 y) = ((h_2 \circ h_1)(x)) \circ_3 ((h_2 \circ h_1)(y))$:

$$(h_2 \circ h_1)(x \circ y) = h_2(h_1(x \circ_1 y)) = h_2(h_1(x) \circ_2 h_1(y)) = h_2(h_1(x)) \circ_3 h_2(h_1(y)) = (h_2 \circ h_1(x)) \circ_3 (h_2 \circ h_1(y))$$

(ii) Zu zeigen ist $\forall y_1, y_2 \in G_2\colon h^{-1}(y_1 \circ_2 y_2) = h^{-1}(y_1) \circ_1 h^{-1}(y_2)$:

$$\exists! x_1, x_2 \in G_1\colon y_1 = h(x_1), y_2 = h(x_2)$$
$$h^{-1}(y_1 \circ_2 y_2) = h^{-1}(h(x_1) \circ_2 h(x_2)) = h^{-1}(h(x_1 \circ_1 x_2)) = x_1 \circ x_2 = h^{-1}(y_1) \circ_1 h^{-1}(y_2)$$

□

Satz 2.6

Seien $(G_1, \circ_1)$ und $(G_2, \circ_2)$ Gruppen und $h\colon G_1 \to G_2$ ein Homomorphismus, dann gilt:
(i) $h(e_1) = e_2$
(ii) $\forall x \in G_1\colon h(x^{-1}) = h(x)^{-1}$

Beweis. (i):

$$h(e_1) = h(e_1) \circ_2 e_2$$
$$h(e_1) = h(e_1 \circ_1 e_1) = h(e_1) \circ_2 h(e_1) = h(e_1) \circ_2 e_2$$
$$\Leftrightarrow h^{-1}(e_1) \circ_2 h(e_1) \circ_2 h(e_1) = h^{-1}(e_1) \circ_2 h(e_1) \circ_2 e_2$$
$$\Leftrightarrow h(e_1) = e_2$$

(ii): Zu zeigen ist $h(x^{-1}) \circ_2 h(x) = e_2 = h(x) \circ_2 h(x^{-1})$:

$$h(x^{-1}) \circ_2 h(x) = h(x^{-1} \circ_1 x) = h(e_1) = e_2 = h(x \circ_1 x^{-1}) = h(x) \circ_2 h(x^{-1})$$

□

2.1.4 Untergruppen

Definition 2.10: Untergruppen

Eine Untergruppe einer Gruppe $(G, \circ)$ ist eine Teilmenge $H \subseteq G, H \neq \emptyset$, sodass
i $\forall x, y \in H\colon x \circ y \in H$
ii $\forall x \in H\colon x^{-1} \in H$
Wir schreiben dann $H \leq G$.

Es sei angemerkt, dass das neutrale Element nicht explizit gefordert wird, weil für $(H, \circ) \leq (G, \cdot)$, weil (i) $e \in H$ und (ii) $H(, \circ)$ eine Gruppe ist.

Beweis. (i) folgt direkt aus der Definition, da $\circ$ über H abgschlossen ist, gilt $x \circ x^{-1} = e \in H$.

(ii) Aus der Definition folgt direkt, dass $\circ$ assoziativ ist und inverse Elemente vorhanden ist. Nach (i) existiert auch ein neutrales Element, somit ist $(H, \circ)$ eine Gruppe. □

2.2 Ringe und Körper

2.2.1 Ringe

Definition 2.11: Ring

Ein Ring $(R, +, \cdot)$ besteht aus einer nichtleeren Menge R und zwei Verknüpfungen $+$ und $\cdot$, sodass:
(R1) $(R, +)$ eine abelsche Gruppe ist
(R2) $(R, \cdot)$ zumindest eine Halbgruppe ist
(R3) Es gelten die Distributivgesetze:
(D1) $\forall x, y, z \in R\colon (x + y) \cdot z = x \cdot z + y \cdot z$
(D1) $\forall x, y, z \in R\colon x \cdot (y + z) = x \cdot y + x \cdot z$
Ein Ring heißt kommutativ, wenn $\cdot$ kommutativ ist. Ist weiters $(R, \cdot)$ ein Monoid, so bezeichnen wir das neutrale Element bzgl. $\cdot$ als 1_R und $(R, +, \cdot)$ als Ring mit 1. Weiters bezeichnen wir das neutrale Element bzgl. $+$ als 0_R und das inverse Element zu $x \in R$ bzgl. $+$ als $-x$. Bezüglich $\cdot$ bezeichnen wir das inverse Element zu $x \in R$ als x^{-1}, sofern es existiert.

- $(\mathbb{Z}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind abelsche Ringe mit 1
- $(\mathbb{N}, +, \cdot)$ ist keine Ring, da $(\mathbb{N}, +)$ keine Gruppe ist
- Sei $\mathbb{R}[x] = \{a_0 + a_1 x + \cdots + a_n x^n | n \in \mathbb{N}_0, a_0, \ldots, a_n \in \mathbb{R}\}$ mit üblichen $+$ und $\cdot$, ist ein abelscher Ringe mit 1, der **Polynomring über** $\mathbb{R}$

Satz 2.7

$(\mathbb{Z}_n, +, \cdot)$ ist ein kommutativer Ring mit 1.

Beweis. Wir wissen bereits, dass $(\mathbb{Z}_n, +)$ eine abelsche Gruppe ist, und $(\mathbb{Z}_n, \cdot)$ ein abelsches Monoid. Wir müssen zeigen, dass die Distributivgesetze gelten.

$$([a]_n + [b]_n) \cdot [c]_n = [a + b]_n \cdot [c]_n = [(a + b) \cdot c]_n = [a \cdot c + b \cdot c]_n$$
$$= [a \cdot c]_n + [b \cdot c]_n = [a]_n \cdot [c]_n + [b]_n \cdot [c]_n$$

Da $\cdot$ auf $\mathbb{Z}_n$ kommutativ ist, genügt es, ein Distributivgesetz zu zeigen. Somit ist $(\mathbb{Z}_n, +, \cdot)$ ein Ring mit 1. □

Definition 2.12: Nullteiler

Ein Element $x \in R \setminus \{0\}$, wobei $(R, +, \cdot)$ ein Ring ist, heißt **Linksnullteiler**, falls $\exists y \in R \setminus \{0\}\colon x \cdot y = 0_R$. Analog heißt x ein **Rechtsnullteiler**, falls $\exists y \in R \setminus \{0\}\colon y \cdot x = 0_R$. Ist x ein Rechts- und Linksnullteiler, so nennen wir x einen Nullteiler.

Betrachten wir ein paar Beispiele. Der Ring $(\mathbb{Z}, +, \cdot)$ ist nullteilerfrei, da $\forall x, y \in \mathbb{Z}\colon x \cdot y = 0 \Leftrightarrow (x = 0 \vee y = 0)$. Allerdings ist $(\mathbb{Z}^2, +, \cdot)$, wobei $+$ und $\cdot$ elementeweise angewendet werden, nicht nullteilerfrei, da z.B. $(0, 1) \cdot (1, 0) = (0, 0)$. Wir wissen bereits, dass $\mathbb{Z}_n$ für gewisse n oftmals mehrere Nullteiler hat. Das ist genau der Fall, wenn n keine Primzahl ist.

Satz 2.8

Sei $n \in \mathbb{P}$, so ist $(\mathbb{Z}_n, +, \cdot)$ nullteilerfrei.

Beweis. Wir wissen, dass $(\mathbb{Z}_n \setminus \{0\}, \cdot)$ eine Gruppe ist. Diese Aussage ist äquivalent dazu, dass $n \in \mathbb{P}$. □

Definition 2.13: Ringhomomorphismen

Seien $(R_1, +_1, \cdot_1)$ und $(R_2, +_2, \cdot_2)$ Ringe. Eine Abbildung $h : R_1 \to R_2$ heißt Ringhomomorphismus, wenn $\forall a, b \in R_1 : h(a +_1 b) = h_(a) +_2 h(b)$ und $\forall a, b \in R_1 : h(a \cdot_1 b) = h(a) \cdot_2 h(b)$.

Ist h ein Ringhomomorphismen, so ist es auch ein Gruppenhomomorphismus bezüglich $+$ und $\cdot$.

Die grundlegende Idee hinter der Algebra ist es, Sätze für Gruppen, Ringe und Körper zu zeigen, um gewisse Eigenschaften in beliebigen Gruppen zu verwenden. Dabei muss dann nur gezeigt werden, dass die Struktur, mit der man arbeitet, eine Gruppe, Ring oder ein Körper ist. Zusätzlich können wir mittels Homomorphismen Eigenschaften auf andere Gruppen übertragen.

2.2.2 Körper

Definition 2.14: Körper

Ein Körper $(K, +, \cdot)$ besteht aus einer Menge K und Verknüpfungen $+$ und $\cdot$, sodass:
(K1) $(K, +)$ eine abelsche Gruppe ist
(K2) $(K \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist
(K3) Es gelten die Distributivgesetze:
(D1) $\forall x, y, z \in K : (a + b)\cdot = a \cdot c + b \cdot c$
Da wir voraussetzen, dass $(K, \cdot)$ abelsch ist, genügt ein Distributivgesetz. Diese Definition ist äquivalent dazu, dass $(K, +, \cdot)$ ein abelscher Ring mit 1 und Inversen ist.

Betrachten wir wieder einige Beispiele. Etwa sind $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ Körper. $(\mathbb{Z}, +, \cdot)$ ist kein Körper, da $(\mathbb{Z} \setminus \{0\}, \cdot)$ keine Gruppe ist, da es kein multiplikatives Inverses gibt. In einem Körper können wir Brüche verwenden:

$$x^{-1} = \frac{1}{x}$$

Auch der Polynomring mit 1 $(\mathbb{R}[x])$ ist kein Körper, da es auch hier kein multiplikatives Inverses gibt. Bildet man einen Ring mit rationalen Funktionen (also x^{-2} usw.), so gibt es ein multiplikatives Inverses, somit handelt es sich ebenfalls um einen Körper. Arbeitet man in $\mathbb{Z}_n$, so ist $(\mathbb{Z}_n, +, \cdot)$ ein Körper, wenn $n \in \mathbb{P}$.

Lemma 2.1

In einem nicht-trivialen Ring mit 1 $(R, +, \cdot)$ $(|R| \geq 2)$ gilt $0 \neq 1$. Weiters gilt, dass das Nullelement eines nicht-trivialen Rings $(R, +, \cdot)$ hat kein multiplikatives Inverses. Zuletzt gilt, dass Körper nullteilerfrei sind.

Beweis. Sei $(R, +, \cdot)$ nicht-trivial, dann $\exists a \in R \setminus \{0\}$, dann $1 \cdot a = a$ und $0 \cdot a = 0$. Daraus folgt $0 \neq 1$. Wir können $0 \cdot a = 0$ verwenden weil:

$$\begin{aligned} & 0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a \\ \Leftrightarrow & 0 \cdot a = 0 \cdot a + 0 \cdot a \\ \Leftrightarrow & 0 \cdot a - 0 \cdot a = 0 \cdot a + 0 \cdot a - 0 \cdot a \\ \Leftrightarrow & 0 = 0 \cdot a \end{aligned}$$

Zuletzt seien $a, b \neq 0$, so wollen wir zeigen, dass $a \cdot b \neq 0$. Wir wissen, dass es multiplikative Inverse zu a und b gibt:

$$a^{-1} \cdot a \cdot b \cdot b^{-1} = 1 \cdot 1 = 1$$

Wäre nun $a \cdot b = 0$, so würde $a^{-1} \cdot a \cdot b \cdot b^{-1} = a^{-1} \cdot 0 \cdot b^{-1} = 0$ gelten. □

Definition 2.15: Körperhomomorphismen

Seien $(K_1, +_1, \cdot_1)$ und $(K_2, +_2, \cdot_2)$ Körper, dann ist eine Abbildung $h : K_1 \to K_2$ ein Körperhomomorphismus, wenn h ein Ringhomomorphismus ist und $h(0_{K_1}) = 0_{K_2}$ und $h(1_{K_1}) = 1_{K_2}$.

Bemerkung 2.1

Für einen Körperhomomorphismus ist $h(0_{K_1}) = 0_{K_2}$ nicht notwendig, weil:

$$h(0_{K_1}) = h(0_{K_1} + 0_{K_1}) = h(0_{K_1}) + h(0_{K_1}) \Rightarrow 0_{K_2} = h(0_{K_1})$$

Allerdings ist $h(1_{K_1}) = 1_{K_2}$ erforderlich, weil:

$$h(1_{K_1}) = h(1_{K_1}) \cdot h(1_{K_1}) \Rightarrow h(1_{K_1})(1_{K_2} - h(1_{K_2})) = 0_{K_2}$$

Wir wissen, dass $(K_2, +_2, \cdot_2)$ nullteilerfrei ist: $h(1_{K_1}) = 0_{K_2}$ oder $h(1_{K_1}) = 1_{K_2}$. $h(1_{K_1}) = 1_{K_2}$. Wenn $h(1_{K_1}) = 0_{K_2}$ dann gilt $h(a) = h(1_{K_1} \cdot_1 a) = h(1_{K_1}) \cdot_2 h(a) = 0_{K_2} \cdot_2 h(a) = 0_{K_2}$ für alle $a \in K_1$. Das Problem hier ist, dass $h(K_1) = \{0_{K_2}\}$, was kein Körper ist. Wir können die zweite Forderung eines Körperhomomorphismus auch ersetzen:

$$h \not\equiv 0 \Leftrightarrow \exists a \in K_1 : h(a) \neq 0_{K_2}$$

Satz 2.9

1) Für jeden Körperhomomorphismus gilt:

$$\forall a \in K_1 : a = 0_{K_1} \Leftrightarrow h(a) = 0_{K_1}$$

2) Weiters gilt, dass jeder Körperhomomorphismus injektiv ist.

Beweis. 1) Folgt aus Bemerkung 2.1:

$$a \neq 0_{K_1} \wedge h(a) = 0_{K_2} \Rightarrow \exists a^{-1} \in K_1 \Rightarrow h(1_{K_1}) = h(a \cdot_1 a^{-1}) = h(a) \cdot_2 h(a^{-1}) = 0_{K_2}$$

2) Sei $h : K_1 \to K_2$ ein Körperhomomorphismus und $a, b \in K_1$ sodass $h(a) = h(b)$. Dann gilt $h(a -_1 b) = h(a) -_2 h(b) = 0_{K_2} \Leftrightarrow a -_1 b = 0_{K_1} \Leftrightarrow a = b$. □

Korollar 2.1

Es gibt einen Körperhomomorphismus von $\mathbb{Z}_p \to \mathbb{Z}_q \Leftrightarrow p = q$. Insbesondere ist der einzige solche Körperhomomorphismus die Identität.

Beweis. Für $p = q$ ist $h : \mathbb{Z}_p \to \mathbb{Z}_q$ die Identität.

Sei $h : \mathbb{Z}_p \to \mathbb{Z}_q$ mit $h([1]_p) = [1]_q$, wobei $h([a]_p) = h(\underbrace{[1]_p + \cdots + [1]_p}_{a \text{ Summanden}}) = a \cdot h([1]_p) = a \cdot [1]_q = [a]_q$. □

Wenn $q < p$, dann ist h nicht injektiv, weil $h([1+q]_p) = h([1]_p)$, wobei aber $[1+q]_p \neq [1]_p$. Wenn $q > p$, dann ist $[1+p]_q = h([1+p]_p) = h([1]_p) = [1]_q$, was ein Widerspruch ist.

2.2.3 Körpererweiterungen

Die Idee hinter Körpererweiterungen ist es, "Zahlen" zu einem Körper hinzuzufügen, um mit diesen "Zahlen" im erweiterten Körper zu rechnen. Wir wissen, dass z.B. die Gleichung $x^2 - 2 = 0$ keine Lösung im Körper $\mathbb{Q}$ hat, da $\sqrt{2}$ irrational ist. Wir betrachten nun $\mathbb{K} = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$. Wir behaupten, dass $(\mathbb{K}, +, \cdot)$ mit den in $\mathbb{R}$ üblichen Operationen $+$ und $\cdot$ ein Körper ist. Wir erben viele nützliche Eigenschaften, wie etwa Assoziativität, neutrale Elemente bezüglich $+$ und $\cdot$, inverse Elemente bezüglich $+$, Distributivgesetze und die Kommutativgesetze. Wir müssen nur überprüfen, ob $+$ und $\cdot$ in $\mathbb{K}$ abgeschlossen sind.

Beweis. Seien $a, b, a', b' \in \mathbb{Q}$, dann gilt: $(a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a + a') + (b + b')\sqrt{2} \in \mathbb{K}$. Und $(a + b\sqrt{2}) \cdot (a' + b'\sqrt{2}) = a \cdot a' + b \cdot b' \cdot 2 + (a \cdot b' + b \cdot a') \cdot \sqrt{2} \in \mathbb{K}$. □

Zuletzt benötigen wir die multiplikativen Inversen für alle $a \in \mathbb{K} \setminus \{0\}$. Wir beginnen:

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \underbrace{\frac{a}{a^2 - 2b^2}}_{\in\mathbb{Q}} - \underbrace{\frac{b}{a^2 - 2b^2}}_{\in\mathbb{Q}} \cdot \sqrt{2} \in \mathbb{K}$$

Oftmals schreiben wir Körpererweiterungen in der Form $\mathbb{Q}(\sqrt{2})$. Wir wissen oben, dass $a^2 - 2b^2$ nicht 0 ist, weil sonst $\frac{a^2}{b^2} = 2$ folgt, dass $\sqrt{2} \in \mathbb{Q}$, was ein Widerspruch ist.

2.2.4 Komplexe Zahlen

Mit der Idee der Körpererweiterungen wollen wir nun das Problem der Gleichung $x^2 + 1 = 0$ angehen. Diese Gleichung hat in $\mathbb{R}$ keine Lösung, da $\forall x \in \mathbb{R}: x^2 \geq 0$. Wir nehmen an, dass eine Zahl i existiert, die $\mathrm{i}^2 = -1$ erfüllt, so gäbe es eine Lösung für die Gleichung. Wir betrachten also die Körpererweiterung $\mathbb{C} = \{a + b\mathrm{i} | a, b \in \mathbb{R}\}$ von $\mathbb{R}$. Wir wollen, dass die folgenden Rechenregeln gelten:

- $(a + b\mathrm{i}) + (c + d\mathrm{i}) = a + c + (b + d)\mathrm{i}$
- $(a + b\mathrm{i}) \cdot (c + d\mathrm{i}) = ac - bd + (ad + bc)\mathrm{i}$
- $\frac{1}{a+b\mathrm{i}} = \frac{a-b\mathrm{i}}{(a+b\mathrm{i})(a-b\mathrm{i})} = \frac{a-b\mathrm{i}}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}\mathrm{i}$

Definition 2.16: Komplexe Zahlen

Mathematisch sind die komplexen Zahlen definiert als $\mathbb{C} = \mathbb{R}^2$ mit den Operationen:

$$(a, b) + (c, d) = (a + c, b + d)$$
$$(a, b) \cdot (c, d) = (ac - bd, ad + bc)$$

Wir schreiben dann anstatt (a, b) $a + b\mathrm{i}$. Diese Darstellung über den $\mathbb{R}^2$ erlaubt es uns, komplexe Zahlen geometrisch zu visualisieren.

Satz 2.10

$(\mathbb{C}, +, \cdot)$ ist ein Körper. Sei $\iota: \mathbb{R} \to \mathbb{C}$ mit $x \mapsto x + 0\mathrm{i}$ ist ein injektiver Körperhomomorphismus (Einbettung). Wir schreiben $\mathbb{R} \subseteq \mathbb{C}$ durch die Einbettung ι.

Beweis. UE: Überprüfen der Körperaxiome □

Definition 2.17

Sei $z \in \mathbb{C}$ mit $z = x + \mathrm{i}y$ heißt $\mathfrak{Re}\{z\} = x$ der Realteil von z, $\mathfrak{Im}\{z\} = y$ der Imaginärteil von z und $\overline{z}$ die zu z konjugiert komplexe Zahl mit $\mathfrak{Re}\{\overline{z}\} = x$ und $\mathfrak{Im}\{\overline{z}\} = -y$.

Wir haben gesehen, dass die Multiplikation von komplexen Zahlen nicht unbedingt "schöne" Ergebnisse liefert. Eine bessere Methode ist es, Multiplikation in Polarkoordinaten durchzuführen. Eine komplexe Zahl z entspricht einem Vektor $(x, y) \in \mathbb{R}^2$. Dieser Vektor hat eine Länge vom Ursprung und einen Winkel zur x-Achse, das Argument. Wir können also eine komplexe Zahl auch über ihren Betrag $|z|$ und ihr Argument $\arg\{z\}$ beschreiben.

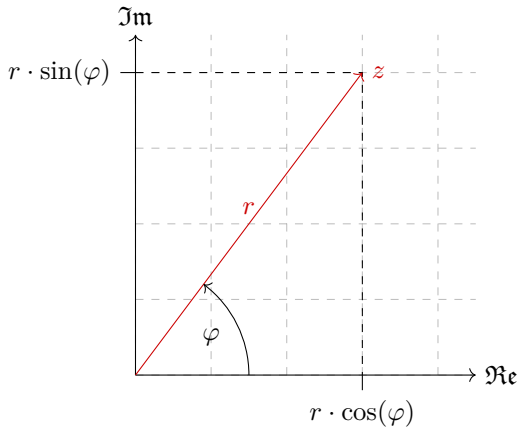

Abbildung 9: Graphische Herleitung der Polarkoordinaten

Es gilt $z = x + \mathrm{i}y = r\cos(\varphi) + \mathrm{i}r\sin(\varphi)$ wobei $r = \sqrt{x^2 + y^2}$ nach dem Satz des Pythagoras und $\tan(\varphi) = \frac{r\sin(\varphi)}{r\cos(\varphi)} = \frac{y}{x}$ wodurch $\varphi = \tan\left(\frac{y}{x}\right) \mod \pi$. Mit der Euler'schen Formel[3] können wir z auch folgendermaßen darstellen:

$$z = r\mathrm{e}^{\mathrm{i}\varphi}$$

Das hat den Vorteil, dass für $z_1 = r_1\mathrm{e}^{\mathrm{i}\varphi_1}$ und $z_2 = r_2\mathrm{e}^{\mathrm{i}\varphi_2}$ das Produkt durch $z_1 z_2 = r_1 r_2 \mathrm{e}^{\mathrm{i}(\varphi_1+\varphi_2)}$ gegeben ist. Bei der Multiplikation werden die Argumente addiert und die Beträge multipliziert. Analog werden bei der Division die Beträge dividiert und die Argumente subtrahiert.

Die Lösungen der Gleichung $x^n - 1 = 0$ heißen n-te Einheitswurzeln:

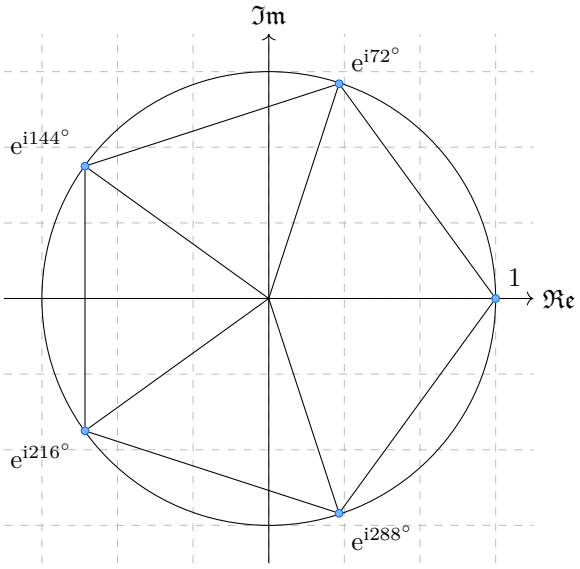

Abbildung 10: Die 5-ten Einheitswurzeln

[3] $\mathrm{e}^{\mathrm{i}\varphi} = \cos(\varphi) + \mathrm{i}\sin(\varphi)$

2.2.5 Vektorräume

Definition 2.18: Vektorraum

Sei $(\mathbb{K}, +, \cdot)$ ein Körper. Ein Vektorraum V über $\mathbb{K}$ ist ein Tripel $(V, \oplus, \odot)$ wobei $V \neq \emptyset$ eine nichtleere Menge $\oplus\colon V \to V$ mit $(v, w) \mapsto v \oplus w$ und $\odot\colon \mathbb{K} \times V \to V$ mit $(\lambda, v) \mapsto \lambda \odot v$ sodass:
(V1) $(V, \oplus)$ eine abelsche Gruppe
(V2) $\odot$ ist assoziativ
(V3) es gelten die die Distributivgestze:
(D1) $\forall \lambda \in \mathbb{K}\colon \forall \boldsymbol{v}, \boldsymbol{w} \in V\colon \lambda \odot (\boldsymbol{v} \oplus \boldsymbol{w}) = \lambda \odot \boldsymbol{v} \oplus \lambda \odot \boldsymbol{w}$
(D2) $\forall \lambda, \mu \in \mathbb{K}\colon \forall v \in V\colon (\lambda + \mu) \odot v = \lambda \odot \boldsymbol{v} \oplus \mu \odot \boldsymbol{v}$

Übliche Beispiele sind etwa $\mathbb{K}^n$ und $\mathbb{K}^{m \times n}$ mit üblichen $+$ und $\cdot$. Etwas abstrakter ist etwa der Raum $\mathbb{K}^X = \{f\colon X \to \mathbb{K}\}$ für eine beliebige Menge X. Hierbei handelt es sich um die Menge aller Funktionen von X nach $\mathbb{K}$. Etwas nützlicher ist $\mathcal{C}([0,1], \mathbb{R})$ die Menge der stetigen Funktionen von $[0,1]$ nach $\mathbb{R}$. Weiters gilt, dass $\mathbb{C}$ ein Vektorraum über $\mathbb{R}$ ist. Allgemein können wir sagen, dass, wenn $\mathbb{K}_1 \subseteq \mathbb{K}_2$, $\mathbb{K}_2$ ein Vektorraum über $\mathbb{K}_1$ ist.

Satz 2.11

Sei $(V, +, \cdot)$ ein Vektorraum über $\mathbb{K}$. Dann gilt:
(i) $\forall \boldsymbol{v} \in V\colon 0\boldsymbol{v} = 0$
(ii) $\forall \lambda \in \mathbb{K}\colon \lambda 0 = 0$
(iii) $\lambda \boldsymbol{v} = 0 \Rightarrow \lambda = 0 \vee \boldsymbol{v} = 0$
(iv) $\forall \boldsymbol{v} \in V\colon (-1) \odot \boldsymbol{v} = -\boldsymbol{v}$

Beweis. Zu (i):

$$0\boldsymbol{v} = (0+0)\boldsymbol{v} = 0\boldsymbol{v} + 0\boldsymbol{v} \Rightarrow 0 = 0\boldsymbol{v}$$

Zu (ii):

$$\lambda 0 = \lambda(0+0) = \lambda 0 + \lambda 0 \Rightarrow 0 = \lambda 0$$

Zu (iii) genügt es zu zeigen, dass $\lambda \neq 0 \Rightarrow \boldsymbol{v} = 0$. Sei $\lambda \neq 0$:

$$\exists \lambda^{-1} \in \mathbb{K} \wedge 0 = \lambda^{-1}(\lambda \boldsymbol{v}) = (\lambda^{-1}\lambda)\boldsymbol{v} = 1\boldsymbol{v} = \boldsymbol{v}xx$$

(iv) Wir zeigen $(-1) \odot \boldsymbol{v} \oplus \boldsymbol{v} = \boldsymbol{v}$:

$$(-1) \odot \boldsymbol{v} \oplus \boldsymbol{v} = (-1) \odot \boldsymbol{v} \oplus (1) \odot \boldsymbol{v} = (-1+1) \odot \boldsymbol{v} = 0 \odot \boldsymbol{v} = 0$$

□

3 Unterräume, lineare Unabhängigkeit und Basen

3.1 Unterräume

Definition 3.1: Unterraum

Eine Teilmenge $U \subseteq V$ eines Vektorraumes $(V, +, \cdot)$ über $\mathbb{K}$ heißt Unterraum oder Teilraum von V, wenn:
(U1) $U \neq \emptyset$
(U2) $\forall \boldsymbol{v}, \boldsymbol{w} \in U : \boldsymbol{v} + \boldsymbol{w} \in U$
(U3) $\forall \lambda \in \mathbb{K} : \forall \boldsymbol{v} \in U : \lambda \boldsymbol{v} \in U$

Beispiele:

- $\{0\}$ und V sind Unterräume von V
- $\mathbb{R}$ und $\mathrm{i}\mathbb{R} = \{\mathrm{i}x | x \in \mathbb{R}\}$ sind Unterräume des Vektorraumes $\mathbb{C}$ über$\mathbb{R}$
- Für jedes $\boldsymbol{v} \in \mathbb{R}^2$ ist $\{\lambda \boldsymbol{v} | \lambda \in \mathbb{K}\}$ ein Unterraum des VR $\mathbb{R}^2$ über $\mathbb{R}$

Satz 3.1: Unterraumkriterium

Sei $U \subseteq V$ ein Unterraum von V. Diese Aussage ist äquivalent dazu, dass $U \neq \emptyset$ und $\forall \boldsymbol{v}, \boldsymbol{w} \in U : \forall \lambda, \mu \in \mathbb{K} : \lambda \boldsymbol{v} + \mu \boldsymbol{w} \in U$.

Beweis. Seien $\boldsymbol{v}, \boldsymbol{w} \in U, \lambda, \mu \in \mathbb{K}$. Dann folgt aus U3, dass $\lambda \boldsymbol{v}, \mu \boldsymbol{w} \in U$ und nach U2 $\lambda \boldsymbol{v} + \mu \boldsymbol{w} \in U$.

Für die Rückrichtung prüfen wir die Unterraumaxiome. U1 ist erfüllt. Für U2 ist $1\boldsymbol{v} + 1\boldsymbol{w} = \boldsymbol{v} + \boldsymbol{w} \in U$, und für U3 ist $\lambda \boldsymbol{v} + 0\boldsymbol{w} = \lambda \boldsymbol{v} \in U$ □

Satz 3.2

Sei $(V, +, \cdot)$ ein VR über $\mathbb{K}$ und $U \subseteq V$ ein Unterraum. Dann ist $(U, +, \cdot)$ ein Vektorraum.

Beweis. Sei $\boldsymbol{v} \in U$, womit $(-1)\boldsymbol{v} = -\boldsymbol{v} \in U \Rightarrow \boldsymbol{v} + (-\boldsymbol{v}) = 0 \in U$. Daher ist $(U, +)$ eine abelsche Gruppe. V2, D1 und D2 werden von V geerbt. □

Beispiele:

- $\mathbb{R}$ ist ein Vektorraume über $\mathbb{Q}$, dann ist $\mathbb{Q}$ ein Unterraum von $\mathbb{R}$
- $V = \mathbb{R}^2$ ist VR über $\mathbb{R}$, $U = \{(x, y) \in \mathbb{R}^2 : x + y = 0\}$ ist ein UR

$$
\begin{aligned}
&(0,0) \in U \Rightarrow U \neq \emptyset \\
&\lambda, \mu \in \mathbb{R}, (x, -x), (y, -y) \in U \Rightarrow \lambda(x, -x) + \mu(y, -y) \\
&= (\lambda x, -\lambda x) + (\mu y, -\mu y) = (\lambda x + \mu y, -\lambda x - \mu y) = (z, -z) \in U
\end{aligned}
$$

- $V = \mathbb{R}^2$, $U = \{(x, y), x + y = 1\}$ ist kein UR, da $(0,0) \notin U$.

Satz 3.3

Sei $(V, +, \cdot)$ ein VR über $\mathbb{K}$, $(U_i)_{i \in I}$ eine Familie von Unterräumen, dann ist $\bigcap_{i \in I} U_i$ ein UR von V.

Beweis. (U1) $\forall i \in I : 0 \in U_i \Rightarrow 0 \in \bigcap_{i \in I} U_i$
(UK) Seien $\lambda, \mu \in \mathbb{K}, \boldsymbol{v}, \boldsymbol{w} \in \bigcap_{i \in I} U_i \Rightarrow \forall i \in I : \boldsymbol{v}, \boldsymbol{w} \in U_i \Rightarrow \forall i \in I : \lambda \boldsymbol{v} + \mu \boldsymbol{w} \in U_i \Rightarrow \lambda \boldsymbol{v} + \mu \boldsymbol{w} \in \bigcap_{i \in I} U_i$. □

Es sei angemerkt, dass $U_1 \cup U_2$, wobei U_1, U_2 UR sind, nicht unbedingt ein UR ist. Seien etwa $U_1 = \{(x, 0), x \in \mathbb{R}\}$ und $U_2 = \{(0, x), x \in R\}$ UR von $\mathbb{R}^2$, dann ist $(1,0) + (0,1) = (1,1)$ nicht in $U_1 \cup U_2$.

3.2 Lineare Hüllen und Basen

Definition 3.2: Erzeugnis

Sei $(V, +, \cdot)$ ein Vektorraum über $\mathbb{K}$ und $M \subseteq V$. Der von M erzeugte Unterraum $[M]$ ist der kleinste Unterraum von V, der M enthält:

$$[M] = \bigcap \{U \subseteq V : U \text{ ist UR}, M \subseteq U\}$$

Eine kleine Bemerkung: Wenn $M = \emptyset$, dann ist $[M] = \{0\}$

Bemerkung 3.1

$[M]$ ist wohldefiniert:
- es gibt mindestens einen Unterraum, der M enthält
- jeder Unterraum, der M enthält, enthält auch $[M]$
- $M \subseteq [M]$, da $M \subseteq U$ für alle U im Durchschnitt
- diese Definitionen sind nicht konstruktiv

Beispiel: $M = \{a\}$ für ein $a \in V$, dann $[M] = \{\lambda a | \lambda \in \mathbb{K}\} = L(a) = \mathcal{L}(a)$. Zu zeigen ist: (i) $[M] \subseteq L(a)$ und (ii) $[M] \supseteq L(a)$.

(ii) $a \in [M] \Rightarrow \forall \lambda \in \mathbb{K}$: $\lambda a \in [M]$ (i) ist klar: $M \subseteq L(a)$, zu zeigen: $L(a)$ ist ein Unterraum. Da $a \in L(a)$ gilt $L(a) \neq \emptyset$. Seien $\boldsymbol{v}, \boldsymbol{w} \in L(a)$ und $\lambda, \mu \in \mathbb{K}$:

$$\begin{aligned} &\exists \alpha, \beta \in \mathbb{K} : \boldsymbol{v} = \alpha a, \boldsymbol{w} = \beta a \\ &\Rightarrow \lambda \boldsymbol{v} + \mu \boldsymbol{w} = \lambda \alpha a + \mu \beta a = \underbrace{(\lambda \alpha + \mu \beta)}_{\in \mathbb{K}} a \end{aligned}$$

Damit ist $L(a)$ ein Unterraum, der M enthält, womit $[M] \subseteq L(a)$

Definition 3.3: Linearkombination und lineare Hülle

Sei V ein Vektorraum über $\mathbb{K}$, $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n \in V$. Eine Linearkombination von $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ ist ein Vektor der Form $\lambda_1 \boldsymbol{a}_1 + \cdots + \lambda_n \boldsymbol{a}_n$ mit $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$.
Für $M \subseteq V$ ist $L(M) = \{\lambda_1 \boldsymbol{a}_1 + \cdots + \lambda_n \boldsymbol{a}_n | n \in N, \lambda_i \in \mathbb{K}, \boldsymbol{a}_i \in M\}$ die Menge der Linearkombinationen von M, oder die Lineare Hülle von M.

Beispiel: $L(\{\boldsymbol{a}, \boldsymbol{b}\})$ ist die von den Vektoren $\boldsymbol{a}, \boldsymbol{b}$ aufgespannte Ebene, wenn $\boldsymbol{a}$ und $\boldsymbol{b}$ linear unabhängig sind.

Satz 3.4: Gleichheit von Erzeugnis und linearer Hülle

Sei $(V, +, \cdot)$ ein Vektorraum über $\mathbb{K}$ und $M \subseteq V$, dann gilt $[M] = L(M)$.

Beweis. Es gilt $M \subseteq L(M)$. Wenn $M = \emptyset$, dann $[M] = \{0\} = L(M)$

(i) $[M] \subseteq L(M)$. Zu zeigen: $L(M)$ ist ein Unterraum:

$$\text{(U1)} : M \neq \emptyset \Rightarrow L(M) \neq \emptyset$$

Seien $\lambda, \mu \in \mathbb{K}$ und $\boldsymbol{v}, \boldsymbol{m} \in L(M)$:

$$\exists \lambda_1, \dots, \lambda_m \in \mathbb{K}\colon \exists \boldsymbol{a}_1, \dots, \boldsymbol{a}_m \in M\colon \boldsymbol{v} = \sum_{k=1}^{m} \lambda_k \boldsymbol{a}_k$$

$$\exists \mu_1, \dots, \mu_n \in \mathbb{K}\colon \exists \boldsymbol{b}_1, \dots, \boldsymbol{b}_n \in M\colon \boldsymbol{w} = \sum_{k=1}^{n} \mu_k \boldsymbol{b}_k$$

$$\Rightarrow \lambda \boldsymbol{v} + \mu \boldsymbol{w} = \lambda \sum_{k=1}^{m} \lambda_k \boldsymbol{a}_k + \mu \sum_{k=1}^{n} \mu_1 \boldsymbol{b}_1$$

$$= \sum_{k=1}^{n} \lambda \lambda_k \boldsymbol{a}_k + \sum_{k=1}^{n} \mu \mu_k \boldsymbol{b}_k \in L(M)$$

(ii) $L(M) \subseteq [M]$. Zu zeigen: Alle Linearkombinationen von M sind in $[M]$ enthalten. Seien $\boldsymbol{a}_1, \dots, \boldsymbol{a}_m \in M$ und $\lambda_1, \dots, \lambda_m \in \mathbb{K}$. Dann folgt aus dem Unterraumkriterium $\sum_{k=1}^{m} \lambda_k \boldsymbol{a}_k \in [M]$. □

Bemerkung 3.2

(i) Für einen Unterraum U gilt $[U] = U = L(U)$. Insbesondere gilt $[[M]] = [M]$ für $M \subseteq V$.
(ii) Auch wenn M unendlich ist schreiben wir Linearkombinationen als endliche Summe $\sum_{\boldsymbol{a} \in M} \lambda_{\boldsymbol{a}} \boldsymbol{a}$ und setzen dabei voraus, dass nur endlich viele $\lambda_{\boldsymbol{a}} \neq 0$.

Beispiel: $V = \mathbb{R}^3$, $\mathbb{K} = \mathbb{R}$ und $M = \{(1,1,1), (0,0,1)\}$:

$$L(M) = \left\{ \lambda_1 \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} + \lambda_2 \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \mid \lambda_1, \lambda_2 \in \mathbb{R} \right\} = \left\{ \begin{bmatrix} \lambda_1 \\ \lambda_1 \\ \lambda_1 + \lambda_2 \end{bmatrix} \mid \lambda_1, \lambda_2 \in \mathbb{R} \right\}$$
$$= \left\{ \begin{bmatrix} \lambda \\ \lambda \\ \mu \end{bmatrix} \mid \lambda, \mu \in \mathbb{R} \right\}$$

Beispiel: $V = \mathbb{Z}_3^3$, $\mathbb{K} = \mathbb{Z}_3$, $M = \{(0,1,0), (1,1,1), (1,0,1)\}$:

$$L(M) = \left\{ \lambda_1 \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + \lambda_2 \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} + \lambda_3 \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \mid \lambda_1, \lambda_2, \lambda \in \mathbb{Z}_3 \right\}$$

$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\} \Rightarrow 3^3$ Kombinationen für $\lambda_1, \lambda_2, \lambda_3$

$$L(M) = \left\{ \begin{bmatrix} \lambda_2 + \lambda_3 \\ \lambda_1 + \lambda_2 \\ \lambda_2 + \lambda_3 \end{bmatrix} \mid \lambda_1, \lambda_2, \lambda_3 \in \mathbb{Z}_3 \right\} = \left\{ (\lambda_1 + \lambda_2) \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + (\lambda_2 + \lambda_3) \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \mid \lambda_1, \lambda_2, \lambda_3 \in \mathbb{Z}_3 \right\}$$

Wenn $\boldsymbol{a} \in L(M)$, dann gilt $L(M) = L(M \cup \{\boldsymbol{a}\})$ und wenn $\boldsymbol{a} \in L(M \setminus \{\boldsymbol{a}\})$, dann gilt $L(M) = L(M \setminus \{\boldsymbol{a}\})$. Das führt uns zu der Frage, ob es minimale Erzeugermengen gibt.

Definition 3.4: Lineare Unabhängigkeit

Sei $(V, +, \cdot)$ ein Vektorraum über $\mathbb{K}$. Ein Tupel $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n) \subseteq V$ heißt linear unabhängig, wenn gilt:

$$\forall \lambda_1, \dots, \lambda_n \in \mathbb{K}\colon \sum_{k=1}^{n} \lambda_k \boldsymbol{v}_k = 0 \Rightarrow \forall k \in \{1, \dots, n\}\colon \lambda_k = 0$$

Andernfalls heißt es linear abhängig.

Eine beliebige Familie $(\boldsymbol{v}_i)_{i \in I}$ heißt linear unabhängig, wenn jedes endliche Tupel $(\boldsymbol{v}_{i_1}, \dots, \boldsymbol{v}_{i_n})$ mit $i_1, \dots, i_n \in I$ linear unabhängig ist. Weiters heißt eine Menge $M \subseteq V$ linear unabhängig, wenn jedes endliche Tupel $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n) \subseteq M$ aus paarweise verschiedenen Elementen linear unabhängig ist. Allgemein bezeichnen wir die

Vektoren $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ als linear unabhängig, anstatt das Tupel $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$. Die leere Familie $(\boldsymbol{v}_i)_{i \in I}$ ist per Definition linear unabhängig.

Weiters sei angemerkt, dass (0) linear abhängig ist, da $\forall \lambda \in \mathbb{K}\colon \lambda 0 = 0$. Damit folgt auch, dass für $\boldsymbol{v}_k = 0$ dann ist $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_k, \dots, \boldsymbol{v}_n)$ linear abhängig, da wir λ_k beliebig wählen können. Wenn $\boldsymbol{v}_k = \lambda \boldsymbol{v}_l$ für ein Paar $k \neq l$ und $\lambda \in \mathbb{K}$, dann ist $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_k, \dots, \boldsymbol{v}_l, \dots, \boldsymbol{v}_n)$ linear abhängig, da wir $\lambda_l = -\lambda$ und $\lambda_k = 1$ wählen um 0 zu erhalten.

Satz 3.5

Seien $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n \in V$, wobei V ein Vektorraum über $\mathbb{K}$ ist, dann sind die folgenden Aussagen äquivalent:

(i) $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ ist linear unabhängig
(ii) $\forall \boldsymbol{v} \in L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n) \exists! \lambda_1, \dots, \lambda_n\colon \boldsymbol{v} = \sum_{k=1}^{n} \lambda_k \boldsymbol{v}_k$
(iii) $\forall k \in \{1, \dots, n\}\colon \boldsymbol{v}_k \notin L(\boldsymbol{v}_1, \dots, \widehat{\boldsymbol{v}_k}, \dots, \boldsymbol{v}_n)$
(iv) $\forall k \in \{1, \dots, n\}\colon L(\boldsymbol{v}_1, \dots, \widehat{\boldsymbol{v}_k}, \dots, \boldsymbol{v}_n) \neq L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$

Beweis. (i) $\Rightarrow$ (ii):

Angenommen, $\boldsymbol{v} \in L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ hat zwei Darstellungen $\boldsymbol{v} = \sum_{k=1}^{n} \lambda_l \boldsymbol{v}_k = \sum_{k=1}^{n} \mu_k \boldsymbol{v}_k$:

$$0 = \boldsymbol{v} - \boldsymbol{v} = \sum_{k=1}^{n} (\lambda_k - \mu_k) \boldsymbol{v}_k \Rightarrow \forall k \in \{1, \dots, k\}\colon \lambda_k - \mu_k = 0 \Leftrightarrow \forall k \in \{1, \dots, n\} \lambda_k = \mu_k$$

(ii) $\Rightarrow$ (iii):

Angenommen $\boldsymbol{v}_k \in L(\boldsymbol{v}_1, \dots, \widehat{\boldsymbol{v}_k}, \dots, \boldsymbol{v}_n) \subseteq L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$, damit aber $\exists \lambda_1, \dots, \widehat{\lambda_k}, \dots, \lambda_n\colon \boldsymbol{v}_k = \lambda_1 \boldsymbol{v}_1 + \dots + 0 \cdot \boldsymbol{v}_k + \dots + \lambda_n \boldsymbol{v}_n = 0 \cdot vecv_1 + \dots + 1 \cdot \boldsymbol{v}_k + \dots + 0 \cdot \boldsymbol{v}_n$. Damit hat $\boldsymbol{v}_k$ zwei verschiedene Darstellungen, was ein Widerspruch zu (ii) ist, somit gilt (iii).

(iii) $\Rightarrow$ (iv)

$\boldsymbol{v}_k \notin L(\boldsymbol{v}_1, \dots, \widehat{\boldsymbol{v}_k}, \dots, \boldsymbol{v}_n) \neq L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$

(iv) $\Rightarrow$ (i)

$L(\boldsymbol{v}_1, \dots, \widehat{\boldsymbol{v}_k}, \dots, \boldsymbol{v}_n) \neq L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$, sprich $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ ist linear unabhängig. Angenommen $\sum_{k=1}^{n} \lambda_k \boldsymbol{v}_k = 0$ mit einem $\lambda_k \neq 0$, somit:

$$\boldsymbol{v}_k = - \sum_{k \in \{1, \dots, \widehat{l}, \dots, n\}} \frac{\lambda_l}{\lambda_k} \boldsymbol{v}_l$$

Dann ist aber $L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n) \subseteq L(\boldsymbol{v}_1, \dots, \widehat{\boldsymbol{v}_k}, \dots, \boldsymbol{v}_n)$. Sei $\boldsymbol{v} \in L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$:

$$\boldsymbol{v} = \mu_1 \boldsymbol{v}_1 + \dots + \mu_k \boldsymbol{v}_k + \mu_n \boldsymbol{v}_n = \mu_1 \boldsymbol{v}_1 + \dots - \frac{\mu_k}{\lambda_k} (\lambda_1 \boldsymbol{v}_1 + \dots + \widehat{\lambda_k \boldsymbol{v}_k} + \dots + \lambda_n \boldsymbol{v}_n) + \mu_{k+1} \boldsymbol{v}_{k+1} + \dots + \mu_n \boldsymbol{v}_n$$

$$= \sum_{l \in \{1, \dots, n\} \setminus \{k\}} \left(\mu_l - \frac{\mu_k \lambda_l}{\lambda_k} \right) \boldsymbol{v}_l \in L(\boldsymbol{v}_1, \dots, \widehat{\boldsymbol{v}_k}, \dots, \boldsymbol{v}_n)$$

Das ist jedoch ein Widerspruch, und somit sind alle Aussagen äquivalent. □

Definition 3.5: Erzeugendensystem

Sei V ein Vektorraum über $\mathbb{K}$:

(i) Eine Familie oder Menge $S \subseteq V$ heißt Erzeugendensystem, wenn $L(S) = V$
(ii) V heißt endlich erzeugt, wenn es ein endliches Erzeugendensystem gibt
(iii) Eine Basis ist ein linear unabhängiges Erzeugendensystem, d.h. eine Familie $(\boldsymbol{b}_i)_{i \in I} \subseteq V$, sodass:
  (a) $(\boldsymbol{b}_i)_{i \in I}$ sind linear unabhängig
  (b) $L(\boldsymbol{b}_i | i \in I) = V$

An dieser Stelle sei angemerkt bzw. wiederholt, dass Linearkombinationen immer endlich sind, sprich wenn $(\boldsymbol{b}_i)_{i \in I}$ eine Basis ist, dann $\forall \boldsymbol{v} \in V\colon \exists i_1, \dots, i_n \in I\colon \exists \lambda_1, \dots, \lambda_n\colon \boldsymbol{v} = \sum_{k=1}^{n} \lambda_1 \boldsymbol{b}_{i_k}$. Weiterhin ist eine beliebige

Familie $(\boldsymbol{u}_i)_{i\in I}$ linear unabhängig, wenn $\forall n\colon \forall i_1,\dots,i_n \in I\colon (\boldsymbol{u}_{i_1},\dots,\boldsymbol{u}_{i_n})$ linear unabhängig ist. Betrachten wir die leere Familie $(\boldsymbol{b}_i)_{i\in\emptyset}$ ist eine Basis von $\{0\}$. Weiterhin, wenn $(\boldsymbol{b}_1,\dots,\boldsymbol{b}_n)$ eine Basis eines Vektorraumes V ist, dann ist auch jede Permutation $(\boldsymbol{b}_{\sigma(i)},\dots,\boldsymbol{b}_{\sigma(n)})$ mit $\sigma\in\mathcal{S}_n$.

Ein klassisches Beispiel für eine Basis ist die Familie der kanonischen Einheitsvektoren über $\mathbb{K}^n$ mit:

$$\boldsymbol{e}_i = \begin{bmatrix} 0\\0\\\vdots\\0\\1\\0\\\vdots\\0 \end{bmatrix}, i=1,\dots,n$$

$$\boldsymbol{x} = \sum_{k=1}^{n} x_k \boldsymbol{e}_k$$

Was passiert nun, wenn wir etwa $V=\mathbb{K}^{\mathbb{N}_0}=\{(a_1,a_2,\dots)|a_i\in\mathbb{K}\}$ (was dem Raum aller Folgen entspricht). Die Einheitsvektoren $\boldsymbol{e}_i=(0,\dots,0,1,0,\dots)$ mit $i\in\mathbb{N}_0$ sind linear unabhängig, aber keine Basis, da nicht jeder Vektor $\boldsymbol{v}\in V$ als (endliche) Linearkombination dargestellt werden kann. $L((\boldsymbol{e}_i)_{i\in\mathbb{N}_0})=\{(a_0,a_1,\dots,a_n,0,0,\dots)|n\in\mathbb{N}_0, a_i\in K, i=0,\dots,n\}$ ist der Raum aller endlichen Folgen, bzw:

$$L((\boldsymbol{e}_i)_{i\in\mathbb{N}_0}) = \bigcup_{n\in\mathbb{N}_0} \mathbb{K}^n$$

Dabei kann diese lineare Hülle als Vektorraum interpretiert werden und mit dem Vektorraum aller Polynome identifiziert werden:

$$\mathbb{K}[x] = \left\{ \sum_{k=0}^{n} a_0 x^k | n\in\mathbb{N}_0, a_k\in\mathbb{K} \right\}$$

Dabei hat $\mathbb{K}[x]$ die Basis $(x^i)_{i\in\mathbb{N}_0}$. In diesem Fall betrachten wir ein Polynom als formalen Ausdruck und nicht als Funktion. Der Grad $\deg(p(x))$ eines Polynoms $p(x)\in\mathbb{K}[x]$ ist $\max\{i|a_i\neg 0\}$, dabei bezeichnet $\mathbb{K}_n[x]$ den Polynomraum, dessen Elemente höchstens Grad n haben, sprich $\mathbb{K}_n[x]=\{p(x)\in\mathbb{K}[x]\colon \deg(p(x))\leq n\}=L(x^0,\dots,x^n)$. Somit gilt:

$$\mathbb{K}[X] = \bigcup_{n\in\mathbb{N}_0} \mathbb{K}_n[x]$$

Wir stellen uns nun die Frage, ob $\mathbb{K}^{\mathbb{N}_0}$ eine Basis hat? Die Antwort ist abhängig vom Auswahlaxiom.

Hat nun jeder Vektorraum eine Basis?

Satz 3.6: Existenz einer Basis

Jeder endlich erzeugte Vektorraum hat eine Basis.

Beweis. Laut Annahme $\exists M=(\boldsymbol{v}_1,\dots,\boldsymbol{v}_n)\colon L(M)=V$. Wenn M linear unabhängig ist, dann ist M eine Basis von V. Wenn dem nicht so ist, dann gilt nach Satz 3.5 (iii), dass $\exists k\in\{1,\dots,n\}\colon \boldsymbol{v}_k\in L(\boldsymbol{v}_1,\dots,\widehat{\boldsymbol{v}_k},\dots,\boldsymbol{v}_n)$. Damit gilt aber $L(\boldsymbol{v}_1,\dots,\widehat{\boldsymbol{v}_k},\dots,\boldsymbol{v}_n)=L(\boldsymbol{v}_1,\dots,\boldsymbol{v}_n)=V$, somit ist $(\boldsymbol{v}_1,\dots,\widehat{\boldsymbol{v}_k},\dots,\boldsymbol{v}_n)$ ein Erzeugendensystem von V.

Wenn $(\boldsymbol{v}_1,\dots,\widehat{\boldsymbol{v}_k},\dots,\boldsymbol{v}_n)$ linear unabhängig ist, haben wir eine Basis. Wenn nicht, entfernen wir einen weiteren linear abhängigen Vektor. Das wiederholen wir so lange, bis die Iteration abbricht. Das geschieht auf jeden Fall, da wir nur endliche Familien betrachten. Der Abbruch geschieht, wenn die verbleibende Familie linear unabhängig ist. □

Exkurs Anfang (nicht prüfungsrelevant)

Hier sehen wir schon das Problem bei unendlich-dimensionalen Vektorräumen. Wenn V nicht endlich erzeugt ist, können wir Satz 3.6 nicht beweisen, da das Entfernen eines Vektors aus einer unendlichen Familie die Familie nicht verkleinert, es ist also nicht garantiert, dass der vorgestellte Algorithmus abbricht. Wir verwenden hierbei eine Eigenschaft der natürlichen Zahlen, dass nämlich jede nichtleere Teilmenge $I \subseteq \mathbb{N}$ ein kleinstes Element hat. Für die reellen Zahlen stimmt das nicht. Betrachten wir $(0,1) = \{x \in \mathbb{R} \colon 0 < x < 1\}$. Dieses offene Intervall hat kein kleinstes Element. Können wir die reellen Zahlen so umordnen, sodass wir zu jeder Teilmenge ein kleinstes Element finden können? Mit dieser Frage hat sich schon Cantor beschäftigt. Eine Menge $(M, \leq)$, wobei $\leq$ eine Totalordnung auf M ist, heißt wohlgeordnet, wenn jede Teilmenge $A \subseteq M$ ein kleinstes Element hat, d.h. $\exists a_0 \in A \colon \forall a \in A \colon a_0 \leq a$. Die natürlichen Zahlen sind wohlgeordnet, die reellen Zahlen jedoch nicht. Cantor hat dann jedoch behauptet, dass jede Menge wohlgeordnet werden kann. Ein Beweis ist erst Zermelo 1905 gelungen. Er hat dabei das Auswahlaxiom verwendet. Sei I eine Indexmenge und $(A_i)_{i \in I}$ eine Familie von Mengen $A_i \neq \emptyset$, dann $\exists (x_i)_{i \in I} \colon \forall i \in I \colon x_i \in A_i$, mit anderen Worten:

$$\bigtimes_{i \in I} A_i \neq \emptyset$$

Eine Folgerung aus dem Auswahlaxiom ist ist das Hausdorff-Banach-Tarski-Paradoxon. Wir betrachten die Sphäre im $\mathbb{R}^3$, sprich $\{(x,y,z) \in \mathbb{R} \colon x^2+y^2+z^2 = 1\} = S^2$. Wir können diese Kugel in fünf disjunkte Teilmengen $S^2 = A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5$ zerlegen, und durch verschieben und drehen zwei Kugeln aus den bestehenden fünf Teilmengen erzeugen. Da das Auswahlaxiom jedoch eine Existenzaussage ist, können wir nicht sagen, von welcher "Form" diese Teilmengen sind. Gödel hat dann 1938 gezeigt, dass, wenn das Zermelo-Fränkel System konsistent ist, dann ist auch das ZF-System mit dem Auswahlaxiom konsistent. 1962 hat weiters Cohen gezeigt, dass auch ZF mit der Verneinung des Auswahlaxioms konsistent ist. Wenn das Auswahlaxiom nicht gilt, dann gibt es endliche Mengen (A_n und (B_n) die jeweils disjunkt sind, mit $|A_n| = |B_n|$, aber $|\bigcup_{n=1}^{\infty} A_n| \neq |\bigcup_{n=1}^{\infty} B_n|$. Eine weiter Frage, die auch von der Verwendung bzw. Akzeptanz des Auswahlaxioms abhängig ist, ist die Frage, ob jeder Vektorraum eine Basis hat. "Glauben" wir an das Auswahlaxiom, so hat jeder Auswahlaxiom eine Basis. Negieren wir das Auswahlaxiom, so gibt es einen Vektorraum ohne Basis.

Das Auswahlaxiom ist äquivalent dazu, dass jede Menge wohlgeordnet werden kann. Eine weitere Äquivalenz besteht zum Lemma von Zorn (1935). Sei $(X, \leq)$ eine totalgeordnete Menge. Wenn jede Kette (d.h. jede totalgeordnete Teilmenge) $A \subseteq X$ eine obere Schranke in X hat, dann $\exists x_0 \in X$ welches ein maximales Element ist. Dabei erfüllt ein maximales Element x_0: $\nexists x \in X \colon x > x_0$ bzw. $\forall x \in X \colon x \leq x_0$ oder aber x ist nicht mit x_0 vergleichbar.

Sei V ein Vektorraum und $X = \{(\boldsymbol{b}_i)_{i \in I} \subseteq V | \text{lineare unabhängige Familien}\}$. Wir betrachten die Relation $(\boldsymbol{b}_i)_{i \in I} \subseteq (\boldsymbol{b}_j)_{j \in J}$. Sei $(B_\alpha)_{\alpha \in A}$ eine totalgeordnete Teilmenge von linear unabhängigen Familien, dann folgt $B_0 = \bigcap_\alpha B_\alpha$ ist eine obere Schranke, somit gibt es ein maximales Element, d.h. es existieren linear unabhängige Familien $(\boldsymbol{b}_i)_{i \in I_0}$, sodass $\forall \boldsymbol{v} \in V \colon (\boldsymbol{b}_i)_{i \in I} \cup \{\boldsymbol{v}\}$ ist nicht linear unabhängig, somit $\boldsymbol{v} \in L((\boldsymbol{b})_{i \in I})$, damit ist $(\boldsymbol{b}_i)_{i \in I}$ eine Basis.

Exkurs Ende

Satz 3.7: Charakterisierung einer Basis

Sei V ein Vektorraum über $\mathbb{K}$, $B = (\boldsymbol{b}_i)_{i \in I}$, dann sind die folgenden Aussagen äquivalent:

(i) B ist eine Basis

(ii) jedes $\boldsymbol{v} \in V$ lässt sich eindeutig als Linearkombination darstellen:

$$\forall \boldsymbol{v} \in V \setminus \{0\} \colon \exists n \in \mathbb{N}_0 \colon \exists! \boldsymbol{b}_{i_1}, \dots, \boldsymbol{b}_{i_n} \in B \colon \exists! \lambda_1, \dots, \lambda_n \colon \lambda_k \neq 0, k \in \{1, \dots, n\} \colon \boldsymbol{v} = \sum_{k=1}^{n} \lambda_k \boldsymbol{b}_{i_n}$$

(iii) B ist eine maximale lineare unabhängige Familie (sprich es gibt keine größere lineare unabhängige Familie (das bedeutet nicht, dass jede andere linear unabhängige Familie darin enthalten ist))

(iv) B ist ein minimales Erzeugendensystem, sprich $\forall \boldsymbol{b} \in B \colon L(B \setminus \{\boldsymbol{b}\}) \neq V$

Beweis. (i) $\Rightarrow$ (ii)

Sei $\boldsymbol{v} \in V$, $\boldsymbol{v} \in L(B)$, angenommen die Darstellung als Linearkombination ist nicht eindeutig:

$$\boldsymbol{v} = \sum_{k=1}^{n} \lambda_k \boldsymbol{b}_{i_k} = \sum_{l=1}^{m} \mu_l \boldsymbol{b}_{i_l}$$

Wobei $I = \{i_1, \dots, i_n\}$ und $J = \{j_1, \dots, j_m\}$. Um etwaige Unterschiede in der Anzahl der Indices auszugleichen ergänzen wir mit 0. Wir nennen $I \cup J = K = \{k_1, \dots, k_p\}$:

$$\boldsymbol{v} = \sum_{l=1}^{p} \lambda_l' \boldsymbol{b}_{k_l} = \sum_{l=1}^{n} \mu_l' \boldsymbol{b}_{k_l}$$

$$\lambda_l' = \begin{cases} \lambda_t & k_l = i_t \\ 0 & \text{sonst} \end{cases} \qquad \mu_l' = \begin{cases} \mu_t & k_l = j_t \\ 0 & \text{sonst} \end{cases}$$

Sprich wir betrachten ohne Beschränkung der Allgemeinheit $m = n$, womit $i_k = j_k, k \in \{1, \dots, k\}$, andernfalls fügen wir die fehlenden $\boldsymbol{b}_j$ mit $0 \cdot \boldsymbol{b}_j$ hinzu:

$$\boldsymbol{v} = \sum_{k=1}^{n} \lambda_k \boldsymbol{b}_{i_k} = \sum_{k=1}^{n} \mu_k \boldsymbol{b}_{i_k}$$

$$\boldsymbol{v} - \boldsymbol{v} = 0 = \sum_{k=1}^{n} (\lambda_k - \mu_k) \boldsymbol{b}_{i_k} \Rightarrow \forall k \in \{1, \dots, n\} \colon \lambda_k - \mu_k = 0 \Leftrightarrow \forall k \in \{1, \dots, n\} \colon \lambda_k = \mu_k$$

Somit ist die Linearkombination eindeutig. Weiter mit (ii) $\Rightarrow$ (i). Klarerweise gilt (ii) $\Rightarrow L(B) = V$. Angenommen $\sum_{k=1}^{n} \lambda_k \boldsymbol{b}_{i_k} = 0 = \sum_{k=1}^{n} 0 \boldsymbol{b}_{i_k}$ woraus folgt $\forall k \in \{1, \dots, n\} \colon \lambda_k = 0$, womit B linear unabhängig ist.

(i) $\Rightarrow$ (iii)

(i) $\Rightarrow B$ ist linear unabhängig. Wenn B maximale ist, gilt $forall \boldsymbol{v} \in V \setminus B \colon B \cup \{v\}$ ist nicht linear unabhängig. Sei $\boldsymbol{v} \in V \setminus B$. Da B eine Basis ist, gilt $\boldsymbol{v} \in L(B) \Rightarrow \exists i_1, \dots, i_n \in I \colon \exists \lambda_1, \dots, \lambda_n \in \mathbb{K} \colon \boldsymbol{v} = \sum_{k=1}^{n} \lambda_k \boldsymbol{b}_{i_k}$. Damit gilt $\sum_{k=1}^{n} \lambda_k \boldsymbol{b}_{i_k} - \boldsymbol{v} = 0$, es gibt also eine Linearkombination von $B \cup \{\boldsymbol{v}\} = 0$, wo nicht alle $\lambda = 0$, womit $B \cup \{\boldsymbol{v}\}$ linear abhängig ist.

(iii) $\Rightarrow$ (iv)

Sei B maximal linear unabhängig. Wir zeigen zuerst $L(B) = \boldsymbol{v}$. Sei $\boldsymbol{v} \in V$. Falls $\boldsymbol{v} \in B$, dann ist $\boldsymbol{v} \in L(B)$. Falls $\boldsymbol{v} \notin B \Rightarrow B \cup \{\boldsymbol{v}\}$ ist linear abhängig. Somit $\exists i_1, \dots, i_n \colon \exists \lambda_0, \lambda_1, \dots, \lambda_n \colon \lambda_0 \boldsymbol{v} + \sum_{k=1}^{n} \lambda_k \boldsymbol{b}_{i_k} = 0$. Wir behaupten nun $\lambda_0 \neq 0$, dann wäre auch $\sum_{k=1}^{n} \lambda_k \boldsymbol{b}_{i_k} = 0$, wenn B linear unabhängig ist, dann ist $\forall k \in \{1, \dots, n\} \colon \lambda_k = 0$, somit $\lambda_0 \neq 0$, womit:

$$\boldsymbol{v} = -\frac{1}{\lambda_0} \left(\sum_{k=1}^{n} \lambda_k \boldsymbol{b}_{i_k} \right) \in L(B)$$

Wir zeigen nun, dass B ein minimales Erzeugendensystem, sprich $\forall \boldsymbol{b} \in B \colon L(B \setminus \{\boldsymbol{b}\}) \neq V$. Angenommen $\exists \boldsymbol{b}_{i_0} \in B \colon \boldsymbol{b}_{i_0} \in L(B \setminus \{\boldsymbol{b}_{i_0}\})$, somit $\exists i_1, \dots, i_n, \lambda_1, \dots, \lambda_n \colon \boldsymbol{b}_{i_0} = \sum_{k=1}^{n} \lambda_1 \boldsymbol{b}_{i_k}$ wobei $0 = -\boldsymbol{b}_{i_0} + \sum_{k=1}^{n} \lambda_k \boldsymbol{b}_{i_k}$, das ist aber eine Linearkombination, bei der $\lambda_0 \neq 0$, was ein Widerspruch dazu ist, dass B linear unabhängig ist.

(iv) $\Rightarrow$ (i)

Angenommen B ist ein minimales Erzeugendensystem, womit $L(B) = V$. Es verbleibt also zu zeigen, dass B linear unabhängig ist. Angenommen $\exists i_1, \dots, i_n \colon \exists (\lambda_1, \dots, \lambda_n) \colon \sum_{k=1}^{n} \lambda_k \boldsymbol{b}_{i_k} = 0$ wobei $(\lambda_1, \dots, \lambda_n) \neq (0, \dots, 0)$, dann folgt $\exists k \colon \lambda_k \neq 0$, ohne Beschränkung der Allgemeinheit wählen wir $\lambda_1 \neq 0$, somit:

$$\boldsymbol{b}_{i_1} = -\frac{1}{\lambda_1} \left(\sum_{k=2}^{n} \lambda_k \boldsymbol{b}_{i_k} \right) \in L(B \setminus \{\boldsymbol{b}_{i_1}\})$$

Mit Satz Satz 3.5 gilt dann $V = L(B) = L(B \setminus \{\boldsymbol{b}_{i_1}\})$, dabei ist $B \setminus \{\boldsymbol{b}_{i_1}\}$ ein kleineres Erzeugendensystem, womit B nicht minimal ist, was ein Widerspruch zu unserer Annahme ist. □

4 Konstruktion von Vektorräumen

Wir haben schon gesehen, wie wir aus einem Vektorraum einen Unterraum erzeugen können. Seien $U, W \subseteq V$ Unterräume, dann ist $U \cap W$ ebenfalls ein Unterraum. Die Vereinigung $U \cup W$ ist im Allgemeinen kein Unterraum. Die lineare Hülle $L(U \cup W)$ hingegen ist ein Unterraum.

Definition 4.1: Summe von Unterräumen

Sei V ein Vektorraum und $U, W \subseteq V$ Unterräume, dann heißt: $U + W = [U \cup W]$ die Summe der Unterräume U und W.

Satz 4.1

Sei V ein Vektorraum und $U, W \subseteq V$ Unterräume, dann gilt:

$$U + W = \{\boldsymbol{u} + \boldsymbol{w} | \boldsymbol{u} \in U, \boldsymbol{w} \in W\}$$

Beweis. Wir zeigen zuerst $[U \cup W] \subseteq \{\boldsymbol{u} + \boldsymbol{w} | \boldsymbol{u} \in U, \boldsymbol{w} \in W\}$. $U + W = [U \cup W] = F$, dabei ist F der kleinste Unterraum, der U und W enthält. Wenn $U + W \subseteq E$, dabei ist E ein Unterraum, der U und W enthält. Klar ist: $U \subseteq E : \boldsymbol{u} = \boldsymbol{u} + 0$ bzw. $W \subseteq E : \boldsymbol{w} = 0 + \boldsymbol{w}$. Seien $\boldsymbol{v}, \boldsymbol{v}' \in E$ mit $\lambda, \mu \in \mathbb{K}$, wir zeigen $\lambda \boldsymbol{v} + \mu \boldsymbol{v}' \in E$:

$$\begin{aligned}
&\boldsymbol{v} \in E \Rightarrow \exists \boldsymbol{u} \in U, \boldsymbol{w} \in W : \boldsymbol{v} = \boldsymbol{u} + \boldsymbol{w} \\
&\boldsymbol{v}' \in E \Rightarrow \exists \boldsymbol{u}' \in U, \boldsymbol{w}' \in W : \boldsymbol{v}' = \boldsymbol{u}' + \boldsymbol{w}' \\
&\lambda \boldsymbol{v} + \lambda \boldsymbol{v}' = \lambda(\boldsymbol{u} + \boldsymbol{w}) + \mu(\boldsymbol{u}' + \boldsymbol{w}') = (\lambda \boldsymbol{u} + \mu \boldsymbol{u}') + (\lambda \boldsymbol{w} + \mu \boldsymbol{w}') \in E
\end{aligned}$$

Wobei $\boldsymbol{u}'' = \lambda \boldsymbol{u} + \mu \boldsymbol{u}' \in U$ und $\boldsymbol{w}'' = \lambda \boldsymbol{w} + \mu \boldsymbol{w}' \in W$ mit $u'' + w'' \in E$.

Weiter zeigen wir, dass E der kleinste Unterraum, der $U \cup W$ enthält, d.h. jeder Unterraum, der $U \cup W$ enthält, enthält auch E. Sei $Z \subseteq V$ ein Unterraum, der $U \cup W$ enthält. Wir zeigen $E \subseteq Z$. Sei $\boldsymbol{v} \in E$, somit $\exists \boldsymbol{u} \in U, \boldsymbol{w} \in W : \boldsymbol{v} = \boldsymbol{u} + \boldsymbol{w}$, wobei $U \subseteq Z$ und $W \subseteq Z$, da Z ein Unterraum ist, ist $\boldsymbol{v} \in Z$, womit $[U \cup W] = \{\boldsymbol{u} + \boldsymbol{w} | \boldsymbol{u} \in U, \boldsymbol{w} \in W\}$ □

Beispiel: Eine (triviale) Beobachtung ist, dass $U + U = [U \cup U] = [U] = U$. Etwas interessanter ist z.B:

$$U = \left\{ \begin{bmatrix} \xi \\ \eta \\ \xi \\ \eta \end{bmatrix} | \xi, \eta \in \mathbb{R} \right\} = L\left(\begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \right)$$

$$W = \left\{ \begin{bmatrix} \xi \\ \xi \\ \eta \\ \eta \end{bmatrix} | \xi, \eta \in \mathbb{R} \right\} = L\left(\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \right)$$

Um $U + W$ zu bestimmen, suchen wir eine Basis von $U + W$:

$$U + W = \{\boldsymbol{u} + \boldsymbol{w} | \boldsymbol{u} \in U, \boldsymbol{w} \in W\} = \left\{ \alpha_1 \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \alpha_2 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} + \alpha_3 \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \alpha_4 \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} | \alpha_i \in \mathbb{R} \right\}$$

$$= L\left(\begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \right)$$

Dabei handelt es sich nicht um eine Basis, da:

$$\begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

Damit ist $U + W$:

$$U + W = L\left(\begin{bmatrix}0\\1\\0\\1\end{bmatrix}, \begin{bmatrix}1\\1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\\1\end{bmatrix}\right)$$

Lemma 4.1

Sei V ein Vektorraum und $M, N \subseteq V$, dann gilt:

$$[M \cup N] = [M] + [N]$$

Beweis. $[M \cup N]$ ist der kleinste Unterraum, der $M \cup N$ enthält.

Klarerweise $[M] \subseteq [M \cup N]$ und $[N] \subseteq [M \cup N]$, womit $[M] + [N] = [[M] \cup [N]] \subseteq [[M \cup N] \cup [M \cup N]] = [[M \cup N]] = [M \cup N]$.

Umgekehrt betrachten wir $[M \cup N] \subseteq [M] + [N]$. Sei $\boldsymbol{v} \in [M \cup N] = L(M \cup N)$, sprich $\exists \boldsymbol{v}_1, \dots, \boldsymbol{v}_m \in M, \boldsymbol{w}_1, \dots, \boldsymbol{w}_n \in \mathbb{N}$: $\exists \lambda_1, \dots, \lambda_m \in \mathbb{K}, \mu_1, \dots, \mu_n \in \mathbb{K}$: $\boldsymbol{v} = \sum_{k=1}^{m} \lambda_k \boldsymbol{v}_k + \sum_{k=1}^{n} \mu_k \boldsymbol{w}_k$, wobei $\sum_{k=1}^{m} \lambda_k \boldsymbol{v}_k \in L(M)$ und $\sum_{k=1}^{n} \mu_k \boldsymbol{w}_k \in L(N)$, und somit $\boldsymbol{v} \in L(M) + L(N) = [L(M) \cup L(N)]$. □

Satz 4.2: Dimensionssatz

Sei V ein Vektorraum und $U, W \subseteq V$ Unterräume mit $\dim(W) < \infty$ und $\dim(U) < \infty$, dann gilt:

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

Beweis. Sei $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_r)$ eine Basis von $U \cap W$. Mit dem Basisergänzungssatz gilt:

$$\exists \boldsymbol{u}_1, \dots, \boldsymbol{u}_p \in U \colon B'(\boldsymbol{v}_1, \dots, \boldsymbol{v}_r, \boldsymbol{u}_1, \dots, \boldsymbol{u}_p)$$
$$\exists \boldsymbol{w}_1, \dots, \boldsymbol{w}_q \in W \colon B'' = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_r, \boldsymbol{w}_1, \dots, \boldsymbol{w}_q)$$

Wobei B' eine Basis von U ist und B'' eine Basis von W ist. Wir behaupten nun, dass

$$B''' = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_r, \boldsymbol{u}_1, \dots, \boldsymbol{u}_p, \boldsymbol{w}_1, \dots, \boldsymbol{w}_q)$$

eine Basis von $U+W$ ist. Wir wissen $\dim(U \cap W) = r$, $\dim(U) = r+p$ und $\dim(W) = r+q$, somit $\dim(U+W) = r + p + q$. Wir zeigen, dass B''' eine Basis ist. Wir wissen $U = L(B')$ und $W = L(B'')$ sowie $U + W = L(B' \cup B'') = L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_r, \boldsymbol{u}_1, \dots, \boldsymbol{u}_p, \boldsymbol{w}_1, \dots, \boldsymbol{w}_q)$. Wir machen einen Zwischenschritt $U \cap L(\boldsymbol{w}_1, \dots, \boldsymbol{w}_q) = \{0\}$. Sei $\boldsymbol{v} \in U \cap L(\boldsymbol{w}_1, \dots, \boldsymbol{w}_q) \subseteq U \cap W = L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_r)$ somit $\boldsymbol{v} \in L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_r) \cap L(\boldsymbol{w}_1, \dots, \boldsymbol{w}_q) = \{0\}$. Angenommen$\boldsymbol{v} \in L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_r) \cap L(\boldsymbol{w}_1, \dots, \boldsymbol{w}_q)$, dann folgt $\boldsymbol{v} = \sum \lambda_i \boldsymbol{v}_i = \sum \mu_j \boldsymbol{w}_j$:

$$\boldsymbol{v} - \boldsymbol{v} = \sum \lambda_i \boldsymbol{v}_i - \sum \mu_j \boldsymbol{w}_j = 0$$

Aber $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_r, \boldsymbol{w}_1, \dots, \boldsymbol{w}_q)$ sind linear unabhängig, sprich alle $\lambda_i =$ und alle $\mu_j = 0$, womit $\boldsymbol{v} = 0$.

B ist linear unabhängig. Seien $\lambda_1, \dots, \lambda_r, \mu_1, \dots, \mu_p, \nu_1, \dots, \nu_q \in \mathbb{K}$, sodass:

$$\sum_{i=1}^{r} \lambda_i \boldsymbol{v}_i + \sum_{j=1}^{p} \mu_j \boldsymbol{u}_j + \sum_{k=1}^{q} \nu_k \boldsymbol{w}_k = 0$$

Wir müssen zeigen, dass alle $\lambda_i = 0$, alle $\mu_j = 0$ und alle $\nu_k = 0$:

$$\boldsymbol{v} = \sum_{i=1}^{r} \lambda_i \boldsymbol{v}_i + \sum_{j=1}^{p} \mu_j \boldsymbol{u}_j = -\sum_{k=1}^{q} \nu_k \boldsymbol{w}_k$$
$$\Rightarrow \boldsymbol{v} \in U \cap L(\boldsymbol{w}_1, \dots, \boldsymbol{w}_q) \Rightarrow \boldsymbol{v} = \boldsymbol{w}$$

Damit gilt $\lambda_i = 0$, $\mu_j = 0$ und $\nu_k = 0$. □

Definition 4.2: Direkte Summe

Die Summe $U + W$ heißt direkt, wenn $\forall \boldsymbol{v} \in U + W \colon \exists! \boldsymbol{u} \in U \colon \exists! \boldsymbol{w} \in W \colon \boldsymbol{v} = \boldsymbol{u} + \boldsymbol{w}$. Wir schreiben $U \dot{+} W$ (oder manchmal $U \oplus W$).

Satz 4.3

Sei V ein Vektorraum und $U, W \subseteq V$ Unterräume. Die Summe $U + W$ ist direkt, wenn gilt:

$$U \cap W = \{0\}$$

Beweis. Angenommen die Summe $U + W$ ist direkt. Sei $\boldsymbol{v} \in U \cap W$:

$$\boldsymbol{v} = \boldsymbol{v} + 0 = 0 + \boldsymbol{v}$$

Wenn die Darstellung eindeutig ist, dann gilt $\boldsymbol{v} = 0$. Umgekehrt gilt $U \cap W = \{0\}$:

$$\boldsymbol{v} = \underbrace{\boldsymbol{a}}_{\in U \cap W} + \underbrace{\boldsymbol{b}}_{\in U} + \underbrace{\boldsymbol{c}}_{\in W}$$

ist eindeutig. Alternativ kann man argumentieren. Sei $\boldsymbol{v} \in U + W$. Angenommen $\boldsymbol{v} = \boldsymbol{u} + \boldsymbol{w}$ und $\boldsymbol{v} = \boldsymbol{u}' + \boldsymbol{w}'$. Wir zeigen $\boldsymbol{u} + \boldsymbol{w} = \boldsymbol{u}' + \boldsymbol{w}'$:

$$\boldsymbol{u} - \boldsymbol{u}' = \boldsymbol{w} - \boldsymbol{w}' \Rightarrow \boldsymbol{u} - \boldsymbol{u}' \in U \cap W \Rightarrow \boldsymbol{u} = \boldsymbol{u}'$$

□

Satz 4.4: Charakterisierung von direkten Summen

Sei $\dim(V) < \infty$ und $U, W \subseteq V$ Unterräume, dann sind die folgenden Aussagen äquivalent:

(i) $V = U \dot{+} W$
(ii) $V = U + W \wedge \dim(V) = \dim(U) + \dim(W)$
(iii) $U \cap W = \{0\} \wedge \dim(V) = \dim(U) + \dim(W)$

Beweis. (i) $\Rightarrow$ (ii)

$V = U \dot{+} W$, dann folgt $V = U + W$ und $U \cap W = \{0\}$ womit nach Satz 4.2 $\dim(V) = \dim(U) + \dim(W) - \underbrace{\dim(U \cap W)}_{=0}$

(ii) $\Rightarrow$ (iii)

wiederum folgt aus Satz 4.2$\dim(V) = \dim(U) + \dim(W) - \dim(U \cap W) \Rightarrow \dim(U \cap W) = 0 \Rightarrow U \cap W = \{0\}$

(iii) $\Rightarrow$ (i)

erneut aus Satz 4.2 $U \cap W = \{0\}$ und $\dim(V) = \dim(U) + \dim(W) = \dim(U + W) + \underbrace{\dim(U \cap W)}_{=0}$, sprich $U + W$ ist ein Unterraum mit $\dim(U + W) = \dim(V)$, somit $U + W = V$. □

Satz 4.5: Komplementärraum

Sei V ein Vektorraum mit $\dim(V) < \infty$. Sei $U \subseteq V$ ein Unterraum, dann $\exists W \subseteq V$ Unterraum, mit $V = U \dot{+} W$. W heißt Komplementärraum.

Beweis. Sei $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n)$ eine Basis von U. Aus dem Basisergänzungssatz folgt: $\exists \boldsymbol{w}_1, \ldots, \boldsymbol{w}_m \in V$, sodass $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n, \boldsymbol{w}_1, \ldots, \boldsymbol{w}_m)$ eine Basis von V ist. Sei $W = L(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m)$, dann ist $V = U \dot{+} W$. Wir müssen also zeigen, dass $U + W = V$ und $U \cap W = \{0\}$. Sei $\boldsymbol{v} \in V$:

$$\boldsymbol{v} = \sum_{i=1}^{n} \lambda_i \boldsymbol{u}_i + \sum_{j=1}^{m} \mu_j \boldsymbol{w}_j \in U + W$$

Sei $\boldsymbol{v} \in U \cap W$, dann $\boldsymbol{v} = \sum_{k=1}^{n} \lambda_i \boldsymbol{u}_i = \sum_{k=1}^{m} \mu_j \boldsymbol{w}_j$:

$$\boldsymbol{v} - \boldsymbol{v} = 0 = \sum_{i=1}^{n} \lambda_i \boldsymbol{u}_i - \sum_{j=1}^{m} \mu_j \boldsymbol{w}_j$$

Da $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_m, \boldsymbol{w}_1, \dots, \boldsymbol{w}_m)$ eine Basis bildet, sind alle $\boldsymbol{u}_i$ und $\boldsymbol{w}_j$ linear unabhängig, somit gilt $\lambda_i = 0$ und $\mu_j = 0$, womit $\boldsymbol{v} = 0$. □

Hier ist zu beachten, dass der Basisergänzungssatz keine eindeutige Basis liefert, sondern nur die Ergänzung einer vorhandenen Basis erlaubt. Somit können wir mit Satz 4.5 auch keinen eindeutigen Komplementärraum W zu einem Unterraum $U \subseteq V$ eines Vektorraumes V ermitteln. Weiterhin ist die Existenz eines Komplementärraums bei unendlich-dimensionalen Vektorraumes V nicht gewährleistet.

Sei V ein Vektorraum und $U_1, \dots, U_m \subseteq V$ Unterräume. Wir betrachten:

$$\sum_{k=1}^{m} U_k = \left[\bigcup_{k=1}^{m} U_k \right] = \left\{ \sum_{k=1}^{m} \boldsymbol{u}_k | \boldsymbol{u}_k \in U_K \right\}$$

Weiters können wir zeigen, dass die Menge aller Unterräume $\mathcal{U}$ mit $+$ ein abelsches Monoid $(\mathcal{U}, +)$ bildet.

Definition 4.3

Die Summe $W = \sum_{k=1}^{m} U_k$ heißt direkt, wenn $\forall \boldsymbol{w} \in W \colon \exists! \boldsymbol{u}_1 \in U_1, \dots, \boldsymbol{u}_m \in U_m \colon \boldsymbol{w} = \sum_{k=1}^{m} \boldsymbol{u}_k$, sprich die Darstellung für $\boldsymbol{w}$ ist eindeutig. Wir schreiben $W = U_1 \dot{+} \cdots \dot{+} U_m$.

Die Abbildungen $\pi_k \colon W \to U_k$ mit $\boldsymbol{w} \mapsto \boldsymbol{u}_k$ heißen Projektionen von W auf U_k. Wir bezeichnen die $\boldsymbol{u}_k$ als "Koordinatenvektoren".

Satz 4.6: Charakterisierung für Direkte Summen

(i) Sei V ein Vektorraum $U_1, \dots, U_m \subseteq V$ nicht-triviale Unterräume. Dann ist die Summe $W = U_1 + \cdots + U_m$ direkt, wenn jede Familie $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_m), \boldsymbol{u}_i \in U_i \setminus \{0\}$ linear unabhängig ist.

Beweis. Seien $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_m), \boldsymbol{u}_i \in U_i \setminus \{0\}$. Seien $\lambda_1, \dots, \lambda_m \in \mathbb{K}$, sodass $\sum_{k=1}^{m} \lambda_k \boldsymbol{u}_k = 0$. Wir müssen zeigen, dass alle $\lambda_i = 0$:

$$0 = \sum_{i=1}^{m} \lambda_i \boldsymbol{u}_i = \sum_{i=1}^{m} \boldsymbol{w}_i$$

Hierbei handelt es sich um eine Zerlegung des Nullvektors, die eindeutig ist. Somit müssen alle $\boldsymbol{w}_i = 0$, womit $\lambda_i = 0 \forall i$.

$\Leftarrow$ Sei $\boldsymbol{w} \in W = U_1 + \cdots + U_m$. Angenommen $\boldsymbol{w} = \boldsymbol{u}_1 + \cdots + \boldsymbol{u}_m$ und $\boldsymbol{w} = \boldsymbol{u}_1' + \cdots + \boldsymbol{u}_m'$. Wir zeigen $\forall i \colon \boldsymbol{u}_i = \boldsymbol{u}_i'$:

$$\begin{aligned} 0 = \boldsymbol{w} - \boldsymbol{w} &= \boldsymbol{u}_1 - \boldsymbol{u}_1' + \cdots + \boldsymbol{u}_m - \boldsymbol{u}_m' \\ &= \sum_{i=1}^{m} (\boldsymbol{u}_i - \boldsymbol{u}_i') \end{aligned}$$

Angenommen $\exists k \colon \boldsymbol{u}_k \neq \boldsymbol{u}_k'$, sprich $\boldsymbol{u}_k - \boldsymbol{u}_k' \neq 0$:

$$\begin{aligned} \boldsymbol{w}_i &= \begin{cases} \boldsymbol{u}_i - \boldsymbol{u}_i' & \boldsymbol{u}_i \neq \boldsymbol{u}_i', \lambda_i = 1 \\ \boldsymbol{u} \in U_i \setminus \{0\} & \boldsymbol{u}_i = \boldsymbol{u}_i', \lambda_i = 0 \end{cases} \\ \Rightarrow \sum_{i=1}^{m} \lambda_i \boldsymbol{w}_i &= \sum_{i=1, \boldsymbol{u}_i \neq \boldsymbol{u}_i'}^{m} \boldsymbol{u}_i - \boldsymbol{u}_i' = \sum_{i=1}^{m} \boldsymbol{u}_i - \boldsymbol{u}_i' = 0 \end{aligned}$$

Nach unserer Voraussetzung sind die $\boldsymbol{w}_i$ linear unabhängig, womit alle $\lambda_i = 0$, womit alle $\boldsymbol{u}_i = \boldsymbol{u}_i'$. □

Satz 4.7

Sei V ein Vektorraum mit $\dim(V) < \infty$ und $U_1, \dots, U_m \subseteq V$ nicht-triviale Unterräume, dann sind die folgenden Aussagen äquivalent:

(i) Die Summe $W = U_1 + \dots U_m$ ist direkt

(ii) Für jede Wahl von Basen $B_i \subseteq U_i, i = 1, \dots, m$ ist $B_1 \cup \dots \cup B_2$ eine Basis von W $\dim(U_1 + \dots + U_m) = \sum_{i=1}^{m} \dim(U_i)$

Beweis. (i) $\Rightarrow$ (ii)

Angenommen $W = U_1 \dot{+} \dots \dot{+} U_m$. Sei $B_i = (\boldsymbol{u}_{i_1}, \dots, \boldsymbol{u}_{i_{r_i}})$ eine Basis von U_i, dann müssen wir zeigen, dass $B_1 \cup \dots \cup B_m$ eine Basis von W ist. Nach Lemma 4.1 ist $L(B_1 \cup \dots \cup B_m) = L(B_1) + \dots + L(B_M) = U_1 + \dots + U_m = W$. Seien $\lambda_{ij} \in \mathbb{K}$, sodass:

$$\sum_{i=1}^{m} \sum_{j=1}^{r_i} \lambda_{ij} \boldsymbol{b}_{i_j} = 0 = \sum_{i=1}^{m} \boldsymbol{w}_i$$

$$\Rightarrow \forall i \colon \sum_{j=1}^{r_i} \lambda_{ij} \boldsymbol{b}_{i_j} = 0$$

Da B_i eine Basis ist, sind $\forall i \colon \lambda_{ij} = 0$ □

Satz 4.8: Fortestzung von Satz 4.6

(ii) Wenn $B_i \subseteq U_i$ eine Basis von $U_i \forall i$ ist, dann ist $B = B_1 \cup \dots \cup B_n$ eine Basis von W.

(iii) $\dim(U_1 + \dots + U_n) = \sum_{i=1}^{n} \dim(U_i)$

Beweis. (i) $\Rightarrow$ (ii)

1) $L(B_1 \cup \dots \cup B_n) = L(B_1) + \dots + L(B_n)$

1. Wenn $\sum_{i=1}^{n} \sum_{j=1}^{r_i} \lambda_{ij} \boldsymbol{b}_{ij} = 0$, wobei $\boldsymbol{u}_i = \sum_{j=1}^{r_i} \lambda_{ij} \boldsymbol{b}_{ij} \in U_i$, dann ist $\sum_{i=1}^{n} \boldsymbol{u}_i = 0 \Rightarrow \forall i \colon \boldsymbol{u}_i = 0$, womit $\forall i \colon \forall \colon \lambda_{ij} = 0$

(ii) $\Rightarrow$ (i)

Wir müssen zeigen: sei $\boldsymbol{w} \in U_1 + \dots + U_n$, so hat w eine eindeutige Darstellung $\boldsymbol{w} = \sum_{i=1}^{n} \boldsymbol{u}_1$ mit $\boldsymbol{u}_i \in U_i$. Angenommen $\boldsymbol{w} = \sum_{i=1}^{n} \boldsymbol{u}_i$ mit $\boldsymbol{u}_i \in U_i$. Sei $B_i \subseteq U_i$ eine Basis mit $B_i = (\boldsymbol{b}_{i_1}, \dots, \boldsymbol{b}_{i_{r_i}})$, dann folgt $\boldsymbol{u}_i = \sum_{j=1}^{r_i} \lambda_{ij} \boldsymbol{b}_{ij}$ und $\boldsymbol{u}_i' = \sum_{j=1}^{r_i} \mu_{ij} \boldsymbol{b}_{ij}$. Sei nun:

$$\boldsymbol{w} = \sum_{i=1}^{n} \sum_{j}^{r_i} \lambda_{ij} \boldsymbol{b}_{ij} = \sum_{i=1}^{n} \sum_{j=1}^{r_i} \mu_{ij} \boldsymbol{b}_{ij}$$

Da $B_1 \cup \dots \cup B_n$ eine Basis von W ist, gilt $\forall i, j \colon \lambda_{ij} = \mu_{ij}$ bzw. $\forall i \colon \boldsymbol{u}_i = \boldsymbol{u}_i'$. □

Betrachten wir nun den $\mathbb{R}^3$. Wir können nun schreiben $\mathbb{R}^3 = U_1 \dot{+} U_2$, wobei wir $U_1 = L(\boldsymbol{e}_1, \boldsymbol{e}_2)$ setzen und $U_2 = L(\boldsymbol{e}_3)$.

$$\mathbb{R}^3 = \left\{ \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} | x_1, x_2, x_3 \in \mathbb{R} \right\} = \left\{ \left(\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \right) | x_1, x_2, x_3 \in \mathbb{R} \right\}$$

Satz 4.9: Äußere Direkte Summe

Seien V, W Vektorräume über $\mathbb{K}$, dann ist:

$$V \times W = \{(\boldsymbol{v}, \boldsymbol{w}) | \boldsymbol{v} \in V, \boldsymbol{w} \in W\}$$

Mit den Operationen:

$$(\boldsymbol{v}, \boldsymbol{w}) + (\boldsymbol{v}', \boldsymbol{w}') = (\boldsymbol{v} + \boldsymbol{v}', \boldsymbol{w} + \boldsymbol{w}')$$
$$\lambda(\boldsymbol{v}, \boldsymbol{w}) = (\lambda \boldsymbol{v}, \lambda \boldsymbol{w})$$

Dann ist $V \times W$ wieder eine Vektorraum mit neutralen Element $(0_V, 0_W)$.

Der Beweis geht analog zu den Beweis, dass $\mathbb{K}^n$ ein Vektorraum ist. Wir bezeichnen die (äußere) direkte Summe zweier Vektorräume V und W mit $V \oplus W$ oder als direktes Produkt.

Sei $V = V_1 \oplus V_2$, dann sind $U_1 = \{(\boldsymbol{v}, 0) | \boldsymbol{v} \in V_1\}$ und $U_2 = \{(0, \boldsymbol{v}) | \boldsymbol{v} \in V_2\}$ Unterräume in V, und es gilt $V = U_1 \dot{+} U_2 = U_1 \oplus U_2$:

$$(\boldsymbol{v}_1, \boldsymbol{v}_2) = (\boldsymbol{v}_1, 0) + (0, \boldsymbol{v}_2)$$

Satz 4.10

Seien V, W endlich-dimensionale Vektorräume, dann gilt $\dim(V \oplus W) = \dim(V) + \dim(W)$.

Beweis. Sei $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_m)$ eine Basis von V und $(\boldsymbol{w}_1, \dots, \boldsymbol{w}_n)$ eine Basis von W, dann ist

$$B = ((\boldsymbol{v}_1, 0), \dots, (\boldsymbol{v}_m, 0), (0, \boldsymbol{w}_1), \dots (0, \boldsymbol{w}_n))$$

eine Basis von $V \oplus W$.

1)

$$L(B) = \left\{ \sum_{i=1}^{m} \lambda_i (\boldsymbol{v}_i, 0) + \sum_{j=1}^{n} \mu_j (0, \boldsymbol{w}_j), \lambda_i, \mu_j \in \mathbb{K} \right\}$$
$$= \left\{ \left(\sum_{i=1}^{m} \lambda \boldsymbol{v}_i, 0 \right) + \left(0, \sum_{j=1}^{n} \mu_j \boldsymbol{w}_j \right), \lambda_i, \mu_j \in \mathbb{K} \right\} = \left\{ \left(\sum_{i=1}^{m} \lambda_i \boldsymbol{v}_i, \sum_{j=1}^{n} \mu_j \boldsymbol{w}_j \right), \lambda_i, \mu_j \in \mathbb{K} \right\}$$
$$= \{(\boldsymbol{v}, \boldsymbol{w}) | \boldsymbol{v} \in V, \boldsymbol{w} \in W\} = V \oplus W$$

2) B ist linear unabhängig. Angenommen:

$$\sum_{i=1}^{m} \lambda_i (\boldsymbol{v}_i, 0) + \sum_{j=1}^{n} \mu_j (0, \boldsymbol{w}_j) = (0, 0)$$
$$= \left(\sum_{i=1}^{n} \lambda_i \boldsymbol{v}_i, \sum_{j=1}^{n} \mu_j \boldsymbol{w}_j \right)$$
$$\Rightarrow \sum_{i=1}^{n} \lambda_i \boldsymbol{v}_i = 0_V \wedge \sum_{j=1}^{n} \mu_j \boldsymbol{w}_j = 0_W$$

Da $\boldsymbol{v}_i$ und $\boldsymbol{w}_j$ jeweils linear unabhängig sind, ist B ebenfalls linear unabhängig. □

Satz 4.11: Verallgemeinertes direktes Produkt und direkte Summe

Sei I eine Indexmenge und V_i ein Vektorraum über $\mathbb{K}$ für $i \in I$. Dann sind:

$$\prod_{i\in I} V_i = \{(\boldsymbol{v}_i)_{i\in I} | \boldsymbol{v}_i \in V_i\} \qquad \text{direktes Produkt}$$
$$\bigoplus_{i\in I} V_i = \{(\boldsymbol{v}_i)_{i\in I} | \boldsymbol{v}_i \in V_i, \text{nur endliche viele} \neq 0\} \qquad \text{direkte Summe}$$

Wenn $|I| \neq \infty$ gilt $\prod_{i\in I} V_i = \bigoplus_{i\in I} V_i$. Für $|I| = \infty$ gilt wiederum $\bigoplus_{i\in I} V_i \subset \prod_{i\in I} V_i$. Mit den Operationen:

$$(\boldsymbol{v}_i)_{i\in I} + (\boldsymbol{w}_i)_{i\in I} = (\boldsymbol{v}_i + \boldsymbol{w}_i)_{i\in I}$$
$$\lambda(\boldsymbol{v}_i)_{i\in I} = (\lambda \boldsymbol{v}_i)_{i\in I}$$

$\prod_{i\in I} V_i$ und $\bigoplus_{i\in I} V_i$ Vektorräume.

Beispiel: $\mathbb{R}^{\mathbb{N}}$ ist ein solcher Vektorraum mit $I = \mathbb{N}$ und $\forall i\colon V_i = \mathbb{R}$, somit ist $\mathbb{R}^{\mathbb{N}}$ die Menge aller Folgen.

$$\bigoplus_{n\in\mathbb{N}} \mathbb{R} = \{(a_i)_{i\in\mathbb{N}} | \text{nur endliche viele } a_i \neq 0\} \simeq \mathbb{R}[x]$$

Zwischen $\bigoplus_{\mathbb{N}} \mathbb{R}$ und $\mathbb{R}^{\mathbb{N}}$ "liegt die Funknationalanalysis". Zum Beispiel der Folgenraum gegeben durch $L^2 = \left\{(a_n)_{n\in\mathbb{N}} | \sum_{n=1}^{\infty} |a_n|^2 < \infty\right\}$ oder $L^1 = \{(a_n)_{n\in\mathbb{N}} | \sum_{n=1}^{\infty} |a_n| < \infty\}$.

Wir wollen nun wieder von $\mathbb{R}^3$ nur auf den $\mathbb{R}^2$ zurückgehen. Sei $V = U \oplus W$. Betrachten wir $P\colon V \to U$ mit $(\boldsymbol{u}, \boldsymbol{w}) \mapsto \boldsymbol{u}$. Wir "vergessen" quais $\boldsymbol{w}$. Betrachten wir $P^{-1}(\boldsymbol{u}) = \{(\boldsymbol{u}, \boldsymbol{w}) | \boldsymbol{w} \in W\} = (\boldsymbol{u}, 0) + \{0\} \times W$. Für den $\mathbb{R}^2$ verwenden wir $(x, y, z) \mapsto (x, y)$. Das Urbild $P^{-1}((x, y)) = \{(x, y, z) | z \in \mathbb{R}\}$. Da für $x \neq 0$ und $y \neq 0$ der Nullvektor bei $z = 0$ nicht in $p^{-1}((x, y))$ enthalten ist, ist $p^{-1}((x, y))$ kein Unterraum.

Satz 4.12

Sei V ein Vektorraum über $\mathbb{K}$ und $U \subseteq V$ ein Unterraum.
(i) Die Relation auf V mit $\boldsymbol{x} \sim_U \boldsymbol{y} \Leftrightarrow \boldsymbol{x} - \boldsymbol{y} \in U$ ist eine Äquivalenzrelation
(ii) Die Äquivalenzklasse eines Vektors $\boldsymbol{v} \in V$ ist gegeben durch:

$$[\boldsymbol{v}]_U = \{\boldsymbol{v} + \boldsymbol{u} | \boldsymbol{u} \in U\}$$

(iii) $\forall \boldsymbol{v}, \boldsymbol{w}, \boldsymbol{v}', \boldsymbol{w}' \in V$ gilt wenn $\boldsymbol{v} \sim_U \boldsymbol{v}'$ und $\boldsymbol{w} \sim_U \boldsymbol{w}'$, dann ist $\boldsymbol{v} + \boldsymbol{w} \sim_U \boldsymbol{v}' + \boldsymbol{w}'$
(iv) $\forall \lambda \in \mathbb{K}$: $\forall \boldsymbol{v}, \boldsymbol{v}' \in V$ mit $\boldsymbol{v} \sim_U \boldsymbol{v}'$ gilt $\lambda \boldsymbol{v} \sim_U \lambda \boldsymbol{v}'$
Wir nennen $[\boldsymbol{v}]_U$ eine lineare Mannigfaltigkeit.

Über nichtlineare[4] Mannigfaltigkeiten reden wir dann in der Differentialgeometrie[5].

Beweis. Zu i) zeigen wir, dass es sich bei $\sim_U$ um eine Äquivalenzrelation handelt.

- reflexiv: $\boldsymbol{v} - \boldsymbol{v} = 0 \in U \Rightarrow \boldsymbol{v} \sim_U \boldsymbol{v}$
- symmetrisch: wenn $\boldsymbol{v} \sim_U \boldsymbol{w} \Rightarrow \boldsymbol{v} - \boldsymbol{w} \in U$, da U ein Unterraum ist, gilt $-(\boldsymbol{v} - \boldsymbol{w}) = \boldsymbol{w} - \boldsymbol{v} \in U \Rightarrow \boldsymbol{w} \sim_U \boldsymbol{v}$
- transitiv: $\boldsymbol{v} \sim_U \boldsymbol{w} \wedge \boldsymbol{w} \sim_U \boldsymbol{z} \Rightarrow \boldsymbol{v} \sim_U \boldsymbol{z}$:

$$\boldsymbol{v} - \boldsymbol{w} \in U \wedge \boldsymbol{w} - \boldsymbol{z} \in U$$
$$\Rightarrow (\boldsymbol{v} - \boldsymbol{w}) + (\boldsymbol{w} - \boldsymbol{z}) = \boldsymbol{v} - \boldsymbol{z} \in U \Rightarrow \boldsymbol{v} \sim_U \boldsymbol{z}$$

Also ist $\sim_U$ eine Äquivalenzrelation.

[4] i.e. allgemein gekrümmt
[5] allgemein handelt es sich bei einer Mannigfaltigkeit um eine Struktur, die lokal euklidisch ist

Zu (ii). Die Äquivalenzklasse $[\boldsymbol{v}]_U = \{\boldsymbol{w} : \boldsymbol{v} \sim_U \boldsymbol{w}\}$:

$$[\boldsymbol{v}]_U = \{\boldsymbol{w} | \boldsymbol{v} - \boldsymbol{w} \in U\} = \{\boldsymbol{w} | \boldsymbol{w} = \boldsymbol{v} - \boldsymbol{u}, \boldsymbol{u} \in U\}$$
$$\{\boldsymbol{w} | \boldsymbol{w} = \boldsymbol{v} + \boldsymbol{u}, \boldsymbol{u} \in U\} = \boldsymbol{v} + U$$

Zu (iii). Sei $\boldsymbol{v} \sim_U \boldsymbol{v}'$ und $\boldsymbol{w} \sim_U \boldsymbol{w}'$, somit $\boldsymbol{u}_1 = \boldsymbol{v} - \boldsymbol{v}' \in U$ und $\boldsymbol{u}_2 = \boldsymbol{w} - \boldsymbol{w}' \in U$:

$$\boldsymbol{u}_1 + \boldsymbol{u}_2 \in U \Leftrightarrow \boldsymbol{v} - \boldsymbol{v}' + \boldsymbol{w} - \boldsymbol{w}' \in U \Leftrightarrow (\boldsymbol{v} + \boldsymbol{w}) - (\boldsymbol{v}' + \boldsymbol{w}') \in U \Rightarrow \boldsymbol{v} + \boldsymbol{w} \sim_U \boldsymbol{v}' + \boldsymbol{w}'$$

Zu (iv): $\boldsymbol{v} \sim_U \boldsymbol{v}'$:

$$\boldsymbol{u} = \boldsymbol{v} - \boldsymbol{v}' \in U$$
$$\Rightarrow \lambda \boldsymbol{u} = \lambda(\boldsymbol{v} - \boldsymbol{v}') = \lambda \boldsymbol{v} - \lambda \boldsymbol{v}' \in U \Rightarrow \lambda \boldsymbol{v} \sim_U \lambda \boldsymbol{v}'$$

□

Satz 4.13: Faktorraum

Sei V ein Vektorraum mit $U \subseteq V$ ein Unterraum, dann ist der Faktorraum $V/U = \{[\boldsymbol{v}]_U, \boldsymbol{v} \in V\} = \{\boldsymbol{v} + U | \boldsymbol{v} \in U\}$ mit den Operationen $[\boldsymbol{v}]_U + [\boldsymbol{w}]_U = [\boldsymbol{v} + \boldsymbol{w}]_U$ und $\lambda[\boldsymbol{v}]_U = [\lambda \boldsymbol{v}]_U$ ist ein Vektorraum mit neutralem Element $[0]_U$.

Wir nennen der Faktorraum auch Quotientenraum. Wir werden sehen $V \simeq V/U \times U$ (daher der Name Faktorraum).

Beweis. Die Addition ist wohldefiniert. Wenn $[\boldsymbol{v}]_U = [\boldsymbol{v}']_U \Rightarrow \boldsymbol{v} \sim_U \boldsymbol{v}'$, und $\boldsymbol{w} \sim_U \boldsymbol{w}'$. Nach Satz 4.12 ist $\boldsymbol{v} + \boldsymbol{w} \sim_U \boldsymbol{v}' + \boldsymbol{w}'$ womit $[\boldsymbol{v} + \boldsymbol{w}]_U = [\boldsymbol{v}' + \boldsymbol{w}']_U$. Die Skalarmultiplikation wird analog bewiesen. Wenn $[\boldsymbol{v}]_U = [\boldsymbol{v}']_U$, dann $\boldsymbol{v} \sim_U \boldsymbol{v}'$ und $\lambda \boldsymbol{v} \sim_u \lambda \boldsymbol{v}'$ und somit $[\lambda \boldsymbol{v}]_U = [\lambda \boldsymbol{v}']_U$.

Das Resultat der Operationen ist also unabhängig vom Repräsentanten der Äquivalenzklasse.

Wir müssen nur noch die Distributivgesetze nachweisen:

$$\lambda([\boldsymbol{v}]_U + [\boldsymbol{w}]_U) = \lambda[\boldsymbol{v} + \boldsymbol{w}]_U = [\lambda(\boldsymbol{v} + \boldsymbol{w})]_U$$
$$= [\lambda \boldsymbol{v} + \lambda \boldsymbol{w}]_U = [\lambda \boldsymbol{v}]_U + [\lambda \boldsymbol{w}]_U = \lambda[\boldsymbol{v}]_U + \lambda[\boldsymbol{w}]_U$$

Die anderen Gesetze werden analog nachgewiesen. □

Beispiel: $V = \mathbb{R}^3$, $U_1 = L((0,0,1))$, dann sind $V_{/U_1}$ alle Geraden in $\mathbb{R}^3$, die parallel zur z-Achse sind. Die Addition zweier Elemente $[\boldsymbol{v}_1]_{U_1}, [\boldsymbol{v}_2]_{U_1} \in V_{/U_1}$ ist dann die Gerade parallel zur z-Achse, die durch den Punkt $\boldsymbol{v}_1 + \boldsymbol{v}_2$ geht.

Betrachten wir $U_2 = L((1,0,0),(0,1,0))$, dann ist $V_{/U_2}$ die Menge aller Ebenen im $\mathbb{R}^3$, die parallel zur xy-Ebene sind. Analog ist $[\boldsymbol{v}_1]_{U_2} + [\boldsymbol{v}_2]_{U_2}$ die zur xy-Ebene parallele Ebene, die durch $\boldsymbol{v}_1 + \boldsymbol{v}_2$ geht.

$\dim(U_1) = 1$ und $\dim(V_{/U_1}) = 2$. Umgekehrt $\dim(U_2) = 2$ und $\dim(V_{/U_2}) = 1$. Wir sehen also: $\dim(V/U) = \dim(V) - \dim(U)$.

Satz 4.14

Sei V ein endlich-dimensionaler Vektorraum mit einem Unterraum U, dann ist $\dim(V/U) = \dim(V) - \dim(U)$.

Beweis. Sei $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r)$ eine Basis von U, dann folgt mit dem Basisergänzungssatz $\exists \boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n-r}$, sodass $B = (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r, \boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n-r})$ eine Basis von V ist. □

Wir behaupten nun, dass $\tilde{B} = ([\boldsymbol{w}_1]_U, \ldots, [\boldsymbol{w}_{n-r}]_U)$ eine Basis von V/U ist. Wir zeigen dazu 1) $L(\tilde{B}) = V/U$ und 2) $\tilde{B}$ ist linear unabhängig.

Zu 1) ist klar, dass $L(\tilde{B}) \subseteq V/U$. Sei $[\boldsymbol{v}]_U \in V/U$ mit Repräsentanten $\boldsymbol{v} \in V$. Somit ist $\boldsymbol{v}$ darstellbar:

$$\begin{aligned}\boldsymbol{v} &= \underbrace{\sum_{i=1}^{r} \lambda_i \boldsymbol{u}_i}_{\in U} + \sum_{j=1}^{n-r} \mu_j \boldsymbol{w}_j \\ \Rightarrow [\boldsymbol{v}]_U &= \sum_{i=1}^{r} \lambda_i [\boldsymbol{u}_i]_U + \sum_{j=1}^{n-r} \mu_j [\boldsymbol{w}_j]_U \\ &= \sum_{i=1}^{r} \lambda_i [0]_U + \sum_{j=1}^{n-r} \mu_j [\boldsymbol{w}_j]_U \in L(\tilde{B})\end{aligned}$$

Somit $L(\tilde{B}) \subseteq V/U$ und $V/U \subseteq L(\tilde{B})$ womit $L(\tilde{B}) = V/U$.

Zu 2). Angenommen:

$$\sum_{j=1}^{n-r} \lambda_j [\boldsymbol{w}_j]_U = [0]_U$$

Wir zeigen, dass alle $\lambda_j = 0$:

$$\begin{aligned}&\sum_{j=1}^{n-r} \lambda_j [\boldsymbol{w}_j]_U = [0]_U \Leftrightarrow \left[\sum_{j=1}^{n-r} \lambda_j \boldsymbol{w}_j\right] = [0]_U \\ &\Rightarrow \sum_{j=1}^{n-r} \lambda_j \boldsymbol{w}_j \sim_U 0 \Rightarrow \sum_{j=1}^{n-r} \lambda_j \boldsymbol{w}_j \in U = L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r) \\ &\Rightarrow \sum_{j=1}^{n-r} \lambda_j \boldsymbol{w}_j \in L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r) \cap L(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n-r}) = \{0\}\end{aligned}$$

Da $W = L(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n-r})$ nach Satz 4.5 komplementär zu U ist, sprich $V = U \dot{+} W$. Da die $\boldsymbol{w}_j$ linear unabhängig sind, gilt $\forall j \colon \lambda_j = 0$.

5 Lineare Abbildungen

Wir erinnern uns an die Gruppentheorie, wo wir Funktionen $f\colon G_1 \to G_2$ betrachtet haben, die die Verknüpfungen erhalten haben. Dabei haben wir den Begriff Homomorphismus kennengelernt, für den gilt $f(x \circ_1 y) = f(x) \circ_2 f(y)$.

Definition 5.1: Lineare Abbildungen

Seien V, W Vektorräume. Eine Abbildung $f\colon V \to W$ heißt linear (oder Vektorraumhomomorphismus), wenn gilt:

$$\forall \boldsymbol{v}, \boldsymbol{w} \in V\colon f(\boldsymbol{v} + \boldsymbol{w}) = f(\boldsymbol{v}) + f(\boldsymbol{w})$$
$$\forall \lambda \in \mathbb{K}\colon \forall \boldsymbol{v} \in V\colon f(\lambda \boldsymbol{v}) = \lambda f(\boldsymbol{v})$$

Wir bezeichnen $L(V, W) = \mathrm{Hom}(V, W) = \{f\colon V \to W, f \text{ linear}\}$.

Satz 5.1

Seien V, W Vektorräume, dann ist $f\colon V \to W$ linear, wenn:

$$\forall \lambda, \mu \in \mathbb{K}\colon \forall \boldsymbol{v}, \boldsymbol{w} \in V\colon f(\lambda \boldsymbol{v} + \mu \boldsymbol{w}) = \lambda f(\boldsymbol{v}) + \mu f(\boldsymbol{w})$$

Beweis. $\Rightarrow$. Seien $\lambda = \mu = 1$, dann ist $f(\lambda \boldsymbol{v} + \mu \boldsymbol{w}) = f(\boldsymbol{v} + \boldsymbol{w})$, was nach Definition $f(\boldsymbol{v}) + f(\boldsymbol{w})$. Sei analog $\boldsymbol{w} = 0$ oder $\mu = 0$, dann gilt $f(\lambda \boldsymbol{v} + \mu \boldsymbol{w}) = f(\lambda \boldsymbol{v}) = \lambda f(\boldsymbol{v})$. □

Beispiel: Die identische Abbildung $\mathrm{id}\colon V \to V$ ist linear. Ein etwas interessanteres Beispiel ist: Sei V ein Vektorraum mit Basis $B = (\boldsymbol{b}_1, \dots, \boldsymbol{b}_n)$. Wir betrachten $\Phi_B\colon V \to \mathbb{K}^n$ mit $\boldsymbol{v} \mapsto (\boldsymbol{v})_B = (\lambda_1, \dots, \lambda_n)$ wobei $\lambda_1, \dots, \lambda_n$ die eindeutigen Koordinaten sind, sodass $\boldsymbol{v} = \sum_{k=1}^n \lambda_k \boldsymbol{b}_k$. Dann ist Φ_B ebenfalls linear. Auch $\Phi_i\colon V \to \mathbb{K}$ mit $\boldsymbol{v} \mapsto \lambda_i$ ist linear. $V = \mathbb{K}^X = \{f\colon X \to \mathbb{K}\}$ ist ein Vektorraum. Für $x \in X$ betrachten wir $\delta_x\colon V \to \mathbb{K}$ mit $f \mapsto f(x)$ mit $f \in V$. δ_x ist linear. Ein Spezialfall hiervon ist $\mathbb{K}^n = \{f\colon \{1, \dots, n\} \to \mathbb{K}\}$.

Betrachten wir $\mathbb{R}[x]$ mit $\frac{\mathrm{d}}{\mathrm{d}x}\colon \mathbb{R}[x] \to \mathbb{R}[x]$ wobei $\sum_{k=1}^n a_k x^k \mapsto \sum_{k=1}^n a_k k x^{k-1}$. Die Abbildung $\frac{\mathrm{d}}{\mathrm{d}x}$ ist linear:

$$\frac{\mathrm{d}}{\mathrm{d}x}(p(x) + q(x)) = \frac{\mathrm{d}}{\mathrm{d}x}p(x) + \frac{\mathrm{d}}{\mathrm{d}x}q(x)$$

Hier ist zu beachten, dass $f\colon \mathbb{R} \to \mathbb{R}$ mit $x \mapsto kx + d$ kann für $d \neq 0$ nicht linear sein, da $f(0 + 0) = f(0) + f(0) = d + d = 2d \neq 0$. Wir betrachten $T_\lambda\colon V \to V$ mit $\boldsymbol{v} \mapsto \lambda \boldsymbol{v}$ ist linear. Weiter gilt für $V = \mathbb{K}^n$ mit fixen $\alpha_1, \dots, \alpha_n \in \mathbb{K}$ mit $T_\alpha\colon \mathbb{K}^n \to \mathbb{K}^n$ wobei $(x_1, \dots, x_n) \mapsto (\alpha_1 x_1, \dots, \alpha_n x_n)$ ist linear. Wir werden sehen, dass fast jede lineare Abbildung diese Gestalt hat. Mit $V = U \dot{+} W$ mit $\boldsymbol{v} = \boldsymbol{u} + \boldsymbol{w}$ eindeutig. $\pi_U\colon V \to U$ wobei $\boldsymbol{v} \mapsto \boldsymbol{u}$ ist linear.

Eine etwas kompliziertere lineare Abbildung ist z.B. eine Drehung im $\mathbb{R}$ um einen Winkel α. Zu beachten ist, dass eine Translation nicht linear ist.

Satz 5.2

Seien V, W Vektorräume und $f\colon V \to W$ linear, dann gilt:

(i) $f(0_V) = 0_W$
(ii) $f(-\boldsymbol{v}) = -f(\boldsymbol{v})$
(iii) $\forall n\colon \forall \lambda_1, \dots, \lambda_n \in V\colon f\left(\sum_{i=1}^n \lambda_i \boldsymbol{v}_i\right) = \sum_{i=1}^n \lambda_i f(\boldsymbol{v}_i)$

Beweis. Zu (i): $f(0) = f(00) = 0f(0) = 0$

Zu (ii): $f(-\boldsymbol{v}) = f(-1\boldsymbol{v}) = -1f(\boldsymbol{v}) = -f(\boldsymbol{v})$

(iii) folgt durch Induktion. □

Definition 5.2: Klassifikation von linearen Abbildungen

Seien V, W Vektorräume über $\mathbb{K}$ und $f \in \mathrm{Hom}(V, w)$. f heißt:
i) Epimorphismus, wenn f surjektiv ist, $f\colon V \twoheadrightarrow W$
ii) Monomorphismus, wenn f injektiv ist, $f\colon V \rightarrowtail W$
iii) Isomorphismus, wenn f bijektiv ist, $f\colon V \xrightarrow{\sim} W$
Ein Isomorphismus $f\colon V \xrightarrow{\sim} V$ heißt Automorphismus. Ein Homomorphismus $f\colon V \to V$ heißt Endomorphismus. Wir nennen $\mathrm{Aut}(V)$ die Menge aller Automorphismen $f\colon V \xrightarrow{\sim} V$ und $\mathrm{End}(V) = \mathrm{Hom}(V, V)$ die Menge aller Endomorphismen $f\colon V \to V$. V ist in W einbettbar, $V \hookrightarrow W$, wenn $\exists f\colon V \rightarrowtail W$. Wir nennen V und W isomorph, $V \simeq W$, wenn $\exists f\colon V \xrightarrow{\sim} W$.

Satz 5.3

Seien U, V, W Vektorräume über $\mathbb{K}$ und $f\colon U \to V$ und $g\colon V \to W$ lineare Funktionen, dann gilt:
(i) $g \circ f\colon U \to W$ ist linear
(ii) Wenn f ein Isomorphismus ist, existiert $f^{-1}\colon W \to V$, und f^{-1} ist ein Isomorphismus

Beweis. Seien $\boldsymbol{v}, \boldsymbol{w} \in U$, $\lambda, \mu \in \mathbb{K}$ und $f \in \mathrm{Hom}(U, V)$ und $g \in \mathrm{Hom}(V, W)$ dann gilt:

$$(g \circ f)(\lambda \boldsymbol{v} + \mu \boldsymbol{w}) = g(f(\lambda \boldsymbol{v} + \mu \boldsymbol{w})) = g(\lambda f(\boldsymbol{v}) + \mu f(\boldsymbol{w})) = g(\lambda f(\boldsymbol{v})) + g(\mu f(\boldsymbol{w}))$$
$$= \lambda g(f(\boldsymbol{v})) + \mu g(f(\boldsymbol{w}))$$

Zu ii) Seien $\lambda, \mu \in \mathbb{K}$ und $\boldsymbol{v}, \boldsymbol{w} \in V$, sei $f\colon U \rightarrowtail V$.

$$f^{-1}(\lambda \boldsymbol{v} + \mu \boldsymbol{w}) = f^{-1}(\lambda f(f^{-1}(\boldsymbol{v})) + \mu f(f^{-1}(\boldsymbol{w}))) = f^{-1}(f(\lambda f^{-1}(\boldsymbol{v}) + \mu f^{-1}(\boldsymbol{w}))) = \lambda f^{-1}(\boldsymbol{v}) + \mu f^{-1}(\boldsymbol{w})$$

□

Satz 5.4

Wir betrachten $\mathrm{Hom}(V, W)$ mit den Operationen $(f + g)(\boldsymbol{v}) = f(\boldsymbol{v}) + g(\boldsymbol{v})$ und $(\lambda f)(\boldsymbol{v}) = \lambda f(\boldsymbol{v})$ ist ein Vektorraum.

Beweis. Wir zeigen die Abgeschlossenheit von $+\colon \mathrm{Hom}(V, W) \times \mathrm{Hom}(V, W) \to \mathrm{Hom}(V, W)$. Wir müssen zeigen, dass $f + g \in \mathrm{Hom}(V, W)$. Seien $\lambda, \mu \in \mathbb{K}$ und $\boldsymbol{v}, \boldsymbol{w} \in V$:

$$(f + g)(\lambda \boldsymbol{v} + \mu \boldsymbol{w}) = f(\lambda \boldsymbol{v} + \mu \boldsymbol{w}) + g(\lambda \boldsymbol{v} + \mu \boldsymbol{w})$$
$$= \lambda f(\boldsymbol{v}) + \mu f(\boldsymbol{w}) + \lambda g(\boldsymbol{v}) + \mu g(\boldsymbol{w}) = \lambda(f(\boldsymbol{v}) + g(\boldsymbol{v})) + \mu(f(\boldsymbol{w}) + g(\boldsymbol{w})) = \lambda(f + g)(\boldsymbol{v}) + \mu(f + g)(\boldsymbol{w})$$

$$(f + g)(\boldsymbol{v}) = f(\boldsymbol{v}) + g(\boldsymbol{v}) = g(\boldsymbol{v}) + f(\boldsymbol{v}) = (g + f)(\boldsymbol{v})$$
$$(f + (g + h))(\boldsymbol{v}) = f(\boldsymbol{v}) + (g + h)\boldsymbol{v} = f(\boldsymbol{v}) + g(\boldsymbol{v}) + h(\boldsymbol{v}) = (f + g)(\boldsymbol{v}) + h(\boldsymbol{v}) = ((f + g) + h)(\boldsymbol{v})$$
$$(f + 0)(\boldsymbol{v}) = f(\boldsymbol{v}) + 0(\boldsymbol{v}) = f(\boldsymbol{v}) + 0 = f(\boldsymbol{v})$$
$$(f + (-f))(\boldsymbol{v}) = f(\boldsymbol{v}) + (-f(\boldsymbol{v})) = 0(\boldsymbol{v}) = 0$$

Und so weiter. □

Satz 5.5

Sei V ein Vektorraum. $(\mathrm{End}(V), +, \circ)$ ist ein Ring mit 1.

Beweis. Wir zeigen noch die Distributivgesetze. Seien $\lambda, \mu \in \mathbb{K}$ und $\boldsymbol{v} \in V$:

$$((f + g) \circ h)(\boldsymbol{v}) = (f + g)(h(\boldsymbol{v})) = f(h(\boldsymbol{v})) + g(h(\boldsymbol{v}))$$
$$(h \circ (f + g))(\boldsymbol{v}) = h((f + g)(\boldsymbol{v})) = h(f(\boldsymbol{v}) + g(\boldsymbol{v})) = h(f(\boldsymbol{v})) + h(g(\boldsymbol{v}))$$

□

Definition 5.3: assoziative Algebra

Eine assoziative Algebra über einem Körper $\mathbb{K}$ ist eine Struktur $(\mathcal{A}, +, \cdot, *)$. Dabei ist $\mathcal{A}$ eine Menge, $+\colon \mathcal{A}^2 \to \mathcal{A}$, $\cdot\colon \mathbb{K} \times \mathcal{A} \to \mathcal{A}$ und $*\colon \mathcal{A}^2 \to \mathcal{A}$, sodass:

1. $(\mathcal{A}, +, \cdot)$ ist ein Vektorraum
2. $(\mathcal{A}, +, *)$ ist ein Ring
3. $\lambda \cdot (\boldsymbol{a} * \boldsymbol{b}) = (\lambda \cdot \boldsymbol{a}) * \boldsymbol{b} = \boldsymbol{a} * (\lambda \cdot \boldsymbol{b})$

Ein Beispiel ist die Algebra der Polynome über $\mathbb{K}[x]$ mit der üblichen Multiplikation:

$$\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{j=0}^{n} b_j x^j\right) = \sum_{i,j} a_i b_j x^{i+j}$$

Satz 5.6

Sei V ein Vektorraum, dann ist $(\mathrm{End}(V), +, \cdot, \circ)$ ist eine $\mathbb{K}$-Algebra.

Da nach Satz 5.4 $(\mathrm{End}(V), +, \cdot)$ ein Vektorraum ist, und nach Satz 5.5 $(\mathrm{End}(V), +, \circ)$ ein Ring mit 1 ist, müssen wir nur noch das neue Distributivgesetz prüfen. Seien $f, g \in \mathrm{End}(V)$, $\boldsymbol{v} \in V$ und $\lambda \in \mathbb{K}$:

$$\lambda((f \circ g)(\boldsymbol{v})) = \lambda(f(g(\boldsymbol{v}))) = \lambda f(g(\boldsymbol{v})) = ((\lambda f) \circ g)(\boldsymbol{v})$$
$$\lambda f(g(\boldsymbol{v})) = f(\lambda g(\boldsymbol{v})) = f(g(\lambda \boldsymbol{v})) = f \circ (\lambda g)(\boldsymbol{v}) = (f \circ (\lambda g))(\boldsymbol{v})$$

Satz 5.7

Seien V, W Vektorräume. Sei $f \in \mathrm{Hom}(V, W)$:

1. $V' \subseteq V$ ein Unterraum, $f(V') \subseteq W$ ist ein Unterraum
2. $W' \subseteq W$ ein Unterraum, $f^{-1}(W') \subseteq V$ ist ein Unterraum

Beweis. Zu (i)

$\forall \boldsymbol{w}_1, \boldsymbol{w}_2 \in f(V')\colon \forall \lambda, \mu \in \mathbb{K}\colon \lambda \boldsymbol{w}_1 + \mu \boldsymbol{w} \in f(V')$. Seien $\boldsymbol{w}_1, \boldsymbol{w}_2 \in f(V')$, dann $\exists \boldsymbol{v}_1, \boldsymbol{v}_2 \in V\colon f(\boldsymbol{v}_1) = \boldsymbol{w}_1, f(\boldsymbol{v}_2) = \boldsymbol{w}_2$, damit $\lambda \boldsymbol{w}_1 + \mu \boldsymbol{w}_2 = \lambda f(\boldsymbol{v}_1) + \mu f(\boldsymbol{v}_2) = f(\lambda \boldsymbol{v}_1 + \mu \boldsymbol{v}_2) \in f(V')$

Zu (ii)

$\forall \boldsymbol{v}_1, \boldsymbol{v}_2 \in f^{-1}(W')\colon \forall \lambda, \mu \in \mathbb{K}\colon \lambda \boldsymbol{v}_1 + \mu \boldsymbol{v}_2 \in f^{-1}(W')$. Seien $\boldsymbol{v}_1, \boldsymbol{v}_2 \in f^{-1}(W')$, dann $f(\boldsymbol{v}_1) \in W'$ und $f(\boldsymbol{v}_2) \in W'$. Da W' ein Unterraum ist, daher gilt $\lambda f(\boldsymbol{v}_1) + \mu f(\boldsymbol{v}_2) \in W'$, womit $f(\lambda \boldsymbol{v}_1 + \mu \boldsymbol{v}_2) \in W' \Leftrightarrow \lambda \boldsymbol{v}_1 + \mu \boldsymbol{v}_2 \in f^{-1}(W')$. □

Satz 5.8

Seien V, W Vektorräume über $\mathbb{K}$ und $f \in \mathrm{Hom}(V, W)$. Wir betrachten $(\boldsymbol{v}_i)_{i \in I} \subseteq V$.

(i) $f(L((\boldsymbol{v})_{i \in I})) = L((f(\boldsymbol{v}_i))_{i \in I})$

(ii) wenn $(f(\boldsymbol{v}_i)_{i \in I})$ linear unabhängig ist, dann ist $(\boldsymbol{v}_i)_{i \in I}$ linear unabhängig

Beweis. Zu (i)

$$\boldsymbol{w} \in f(L((\boldsymbol{v}_i)_{i \in I})) \Leftrightarrow \exists \boldsymbol{v} \in L((\boldsymbol{v}_i)_{i \in I})\colon \boldsymbol{w} = f(\boldsymbol{v})$$
$$\Leftrightarrow \exists n \in \mathbb{N}\colon \exists i_1, \dots i_n \in I\colon \exists \lambda_1, \dots, \lambda_n \in \mathbb{K}\colon \boldsymbol{w} = f\left(\sum_{k=1}^{n} \lambda_K \boldsymbol{v}_{i_k}\right) = \sum_{k=1}^{n} \lambda_k f(\boldsymbol{v}_{i_k})$$
$$\Leftrightarrow \boldsymbol{w} \in L((f(\boldsymbol{v}_i))_{i \in I})$$

Zu (ii)

Angenommen $\sum_{k=1}^{n} \lambda_k \boldsymbol{v}_{i_k} = 0$, dann müssen alle $\lambda_k = 0$:

$$f\left(\sum_{k=1}^{n} \lambda_k \boldsymbol{v}_{i_k}\right) = \sum_{k=1}^{n} \lambda_k f(\boldsymbol{v}_{i_k}) = 0$$
$$\Rightarrow \lambda_k = 0, k = 1, \ldots, n$$

□

Korollar 5.1

Seien V, W Vektorräume über $\mathbb{K}$ und $f \in \mathrm{Hom}(V, W)$:
- i $f\colon V \twoheadrightarrow W$ und $L(M) = V \Rightarrow L(f(M)) = W$
- ii $f\colon V \rightarrowtail W$ und $M \subseteq V$ linear unabhängig, dann ist $f(M)$ linear unabhängig
- iii $f\colon V \rightarrowtail\!\!\!\!\twoheadrightarrow W$ und B eine Basis von V, dann ist $f(B)$ eine Basis von W

Beweis. Es verbleibt nur noch (ii) zu zeigen. Angenommen $\sum_{k=1}^{n} \lambda_k f(\boldsymbol{v}_{i_k}) = 0$. Wir zeigen $\forall k\colon \lambda_k = 0$:

$$\sum_{k=1}^{n} \lambda_k f(\boldsymbol{v}_{i_k}) = 0$$
$$\Rightarrow f\left(\sum_{k=1}^{n} \lambda_k \boldsymbol{v}_{i_K}\right) = 0 = f(0)$$
$$\Rightarrow \sum_{k=1}^{n} \lambda_k \boldsymbol{v}_{i_k} = 0 \Rightarrow \forall k\colon \lambda_k = 0$$

Das gilt, da die $\boldsymbol{v}_{i_k}$ linear unabhängig sind. □

Satz 5.9

Seien V, W Vektorräume und $f \in \mathrm{Hom}(V, W)$:
- i $f\colon V \rightarrowtail W \Rightarrow \dim(V) \leq \dim(W)$
- ii $f\colon V \twoheadrightarrow W \Rightarrow \dim(V) \geq \dim(W)$
- iii $f\colon V \rightarrowtail\!\!\!\!\twoheadrightarrow W \Rightarrow \dim(V) = \dim(W)$

Beweis. Sei $(\boldsymbol{b}_i)_{i \in I}$ eine Basis von V.

Zu (i)

Sei f injektiv, dann ist $(f(\boldsymbol{b}_i))_{i \in I}$ ist linear linear unabhängig in W, womit $\dim(W) \geq |I| = \dim(V)$.

Zu (ii)

Sei f surjektiv, dann ist $L((f(\boldsymbol{v}_i))_{i \in I}) = W$, womit $|I| \geq \dim(W)$.

(iii) folgt aus (i) und (ii) □

Wir nennen die Dimension eine Invariante unter Isomorphismen.

Satz 5.10: Fortsetzungssatz für lineare Abbildungen

Seien V, W Vektorräume über $\mathbb{K}$, $(\boldsymbol{b}_i)_{i \in I}$ eine Basis von V und $(\boldsymbol{w}_i)_{i \in I} \subseteq W$, dann $\exists! f \in \mathrm{Hom}(V, W)\colon \forall i \in I\colon f(\boldsymbol{b}_i) = \boldsymbol{w}_i$.

Daraus folgern wir, dass zwei lineare Abbildungen $f, g\colon V \to W$ sind gleich, wenn $(f(\boldsymbol{b}_i))_{i \in I} = (g(\boldsymbol{b}_i))_{i \in I}$.

Beweis. Für $\boldsymbol{v} \in V$. Sei $\boldsymbol{v} = \sum_{j=1}^{n} \alpha_j \boldsymbol{b}_{i_j}$. Wir definieren $f(\boldsymbol{v}) = \sum_{j=1}^{n} \alpha_j \boldsymbol{w}_{i_j}$, dabei ist f wohldefiniert, da die Darstellung von $\boldsymbol{v}$ eindeutig ist. Und es gilt $f(\boldsymbol{b}_i) = \boldsymbol{w}_i$, da $\boldsymbol{b}_i = 1\boldsymbol{b}_i$.

Wir zeigen nun, dass f linear ist. Sei $\boldsymbol{u} = \sum_{j=1}^{n} \alpha_j \boldsymbol{b}_{i_J}$ und $\boldsymbol{v} = \sum_{j=1}^{n} \beta_j \boldsymbol{b}_{i_j}$, dann ist:

$$f(\lambda\boldsymbol{u} + \mu\boldsymbol{v}) = f\left(\sum_{j=1}^{n} \lambda\alpha_j \boldsymbol{b}_{i_j} + \sum_{j=1}^{n} \mu\beta_j \boldsymbol{b}_{i_j}\right)$$
$$= f\left(\sum_{j=1}^{n} (\lambda\alpha_j + \mu\beta_j)\boldsymbol{b}_{i_j}\right) = \sum_{j=1}^{n} (\lambda\alpha_j + \mu\beta_j)\boldsymbol{w}_{i_j} = \lambda \sum_{j=1}^{n} \alpha_j \boldsymbol{w}_{i_j} + \mu \sum_{j=1}^{n} \mu_j \boldsymbol{w}_{i_j} = \lambda f(\boldsymbol{u}) + \mu f(\boldsymbol{v})$$

Und zuletzt die Eindeutigkeit. Sei $g\colon V \to W$ eine weitere lineare Abbildung mit $\forall i \in I\colon g(\boldsymbol{b}_i) = \boldsymbol{w}_i$. Sei $\boldsymbol{v} = \sum_{j=1}^{n} \alpha_j \boldsymbol{b}_{i_j}$:

$$g(\boldsymbol{v}) = g\left(\sum_{j=1}^{n} \alpha_j \boldsymbol{b}_{i_j}\right) = \sum_{j=1}^{n} \alpha_j g(\boldsymbol{b}_{i_j}) = \sum_{j=1}^{n} \alpha_j \boldsymbol{w}_{i_j} = f(\boldsymbol{v})$$

□

Satz 5.11

Wenn $\dim(V), \dim(W) < \infty$ Vektorräume sind, dann ist $V \simeq W \Leftrightarrow \dim(V) = \dim(W)$.

Beweis. $\Rightarrow$ haben wir bereits bewiesen. Wir zeigen noch $\Leftarrow$.

Sei $\dim(V) = \dim(W) = n$. Sei $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ eine Basis von V und $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n)$ eine Basis von W. Sei $f\colon V \to W$ die nach Satz 5.10 eindeutige lineare Abbildung mit der Eigenschaft $f(\boldsymbol{v}_i) = f(\boldsymbol{w}_i)$. Wir zeigen nun, f ist ein Isomorphismus. Wir prüfen zuerst, ob f injektiv. Angenommen $f(\boldsymbol{v}) = f(\boldsymbol{v}')$ für $\boldsymbol{v}, \boldsymbol{v}' \in V$:

$$\boldsymbol{v} = \sum_{i=1}^{n} \lambda_i \boldsymbol{v}_i \qquad \boldsymbol{v}' = \sum_{i=1}^{n} \mu_i \boldsymbol{v}_i$$
$$f(\boldsymbol{v}) = \sum_{i=1}^{n} \lambda_i \boldsymbol{w}_i \qquad f(\boldsymbol{v}') = \sum_{i=1}^{n} \mu_i \boldsymbol{w}_i$$
$$0 = f(\boldsymbol{v}) - f(\boldsymbol{v}') = \sum_{i=1}^{n} (\lambda_i - \mu_i)\boldsymbol{w}_i$$

Da die $(\boldsymbol{w}_i)$ eine Basis bilden, muss gelten $\lambda_i = \mu_i$, womit $\boldsymbol{v} = \boldsymbol{v}'$.

Zur Surjektivität. Sei $\boldsymbol{w} \in W$. Mit der Basis von W gilt:

$$\exists \lambda_1, \ldots, \lambda_n\colon \boldsymbol{w} = \sum_{i=1}^{n} \lambda_i \boldsymbol{w}_i$$
$$= \sum_{i=1}^{n} \lambda_i f(\boldsymbol{v}_i) = f\left(\sum_{i=1}^{n} \lambda_i \boldsymbol{v}_i\right)$$

□

Korollar 5.2

$\dim(V) = n \Leftrightarrow V \simeq \mathbb{K}^n$

Beweis. Sei $(\boldsymbol{b}_i)$ eine Basis von V, dann ist $f(\boldsymbol{b}_i) = \boldsymbol{e}_i$ für $i = 1, \ldots, n$. f ist ein Isomorphismus. Umgekehrt, sei $g\colon \mathbb{K}^n \twoheadrightarrow V$, dann ist $\boldsymbol{b}_i = g(\boldsymbol{e}_i)$ eine Basis von V. □

Satz 5.12

Seien V, W $\mathbb{K}$-Vektorräume mit $\dim(V), \dim(W) < \infty$. $\mathrm{Hom}(V, W)$ mit den üblichen Operationen ist ein Vektorraum über $\mathbb{K}$. Es gilt $\dim(\mathrm{Hom}(V, W)) = \dim(V)\dim(W)$.

Beweis. Wir konstruieren eine Basis. Sei $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ eine Basis von V und $(\boldsymbol{w}_1, \dots, \boldsymbol{w}_m)$ eine Basis von W. Sei für $1 \leq i \leq m$ und $1 \leq j \leq n$ $f_{ij} \colon V \to W$ mit:

$$\boldsymbol{v}_k \mapsto \begin{cases} \boldsymbol{w}_j & k = j \\ 0 & k \neq j \end{cases} \Leftrightarrow f_{ij}(\boldsymbol{v}_k) = \boldsymbol{w}_i \delta_{jk}$$

Bei δ_{jk} handelt es sich um das Kronecker-Delta[6].

Wir behaupten nun $B = (f_{ij})$ mit $1 \leq i \leq m$ und $1 \leq j \leq n$ ist eine Basis von $\mathrm{Hom}(V, W)$.

(i) B ist linear unabhängig. Sei $f = \sum_{i=1}^{m} \sum_{j=1}^{n} \lambda_{ij} f_{ij} = 0$, dann ist zu zeigen, dass alle $\lambda_{ij} = 0$, sprich $\forall \boldsymbol{v} \in V \colon f(\boldsymbol{v}) = 0$. Insbesondere ist $\forall k \in \{1, \dots, n\} \colon f(\boldsymbol{v}_k) = 0$:

$$0 = f(\boldsymbol{v}_k) = \sum_{i,j} \lambda_{ij} f_{ij}(\boldsymbol{v}_k) = \sum_{i=1}^{m} \lambda_{ik} f_{ik}(\boldsymbol{v}_k) = \sum_{i=1}^{m} \lambda_{ik} \boldsymbol{w}_i$$

Da die $\boldsymbol{w}_i$ linear unabhängig sind, folgt $\lambda_{ik} = 0$ für $i = 1, \dots, m$. Somit sind alle $\lambda_{ij} = 0$.

(ii) Jede lineare Abbildung $f \colon V \to W$ ist eine Linearkombination der f_{ij}. Wir verwenden erneut Satz 5.10. Sei $f \in \mathrm{Hom}(V, W)$ und:

$$g = \sum_{i=1}^{m} \sum_{j=1}^{m} \lambda_{ij} f_{ij}$$

$f = g \Leftrightarrow \forall k \in \{1, \dots, n\} \colon f(\boldsymbol{v}_k) = g(\boldsymbol{v}_k)$ wir betrachten also die $f(\boldsymbol{v}_k)$. Sei $1 \leq k \leq n$. Es gilt $f(\boldsymbol{v}_k) \in W$, dann:

$$\exists! \alpha_{1k}, \dots, \alpha_{mk} \colon f(\boldsymbol{v}_k) = \sum_{i=1}^{m} \alpha_{ik} \boldsymbol{w}_i$$

Sei $g = \sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_{ij} f_{ij}$. Wir behaupten nun $f = g$.

$$g(\boldsymbol{v}_k) = \sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_{ij} f_{ij}(\boldsymbol{v}_k) = \sum_{i=1}^{n} \alpha_{ik} \boldsymbol{w}_i = f(\boldsymbol{v}_k)$$

□

Definition 5.4: Kern

Sei $f \in \mathrm{Hom}(V, W)$, dann heißt
- i $\ker(f) = f^{-1}(\{0\}) = \{v \in V | f(\boldsymbol{v}) = 0\}$ der Kern von f
- ii $\mathrm{im}(f) = \mathrm{ran}(f) = f(V)$ heißt Bild von f

Beispiel: $f \colon \mathbb{K}^n \to \mathbb{K}^n$:

$$(x_1, \dots, x_n) \mapsto (x_1, \dots, x_m, 0, \dots, 0)$$

$\mathrm{im}(f) = L(\boldsymbol{e}_1, \dots, \boldsymbol{e}_m)$ und $\ker(f) = L(\boldsymbol{e}_{m+1}, \dots, \boldsymbol{e}_n)$. In diesem Beispiel gilt sogar $\ker(f) \dot{+} \mathrm{im}(f) = \mathbb{K}^n$. Allgemein gilt $\dim(\ker(f)) + \dim(\mathrm{im}(f)) = \dim(V)$.

[6] $\delta_{jk} = \begin{cases} 1 & j = k \\ 0 & j \neq k \end{cases}$

Satz 5.13

Sei $f \in \mathrm{Hom}(V,W)$, dann:
i $f\colon V \twoheadrightarrow W \Leftrightarrow \mathrm{im}(f) = W$
ii $f\colon V \rightarrowtail W \Leftrightarrow \ker(f) = \{0\}$

Beweis. (i) ist trivial durch die Definition der Surjektivität erfüllt

Zu (ii)

$\Rightarrow$ Wenn $\boldsymbol{v} \in \ker(f)$, dann $f(\boldsymbol{v}) = 0 = f(0)$, da f injektiv ist, gilt $\boldsymbol{v} = 0$.

$\Leftarrow$ Angenommen $\ker(f) = \{0\}$. Wenn $f(\boldsymbol{v}) = f(\boldsymbol{v}')$, sprich $f(\boldsymbol{v}) - f(\boldsymbol{v}') = 0$, dann $f(\boldsymbol{v} - \boldsymbol{v}') = 0$ womit $\boldsymbol{v} - \boldsymbol{v}' \in \ker(f)$, womit $\boldsymbol{v} - \boldsymbol{v}' = 0 \Leftrightarrow \boldsymbol{v} = \boldsymbol{v}'$, somit ist f injektiv. □

Satz 5.14

Seien V, W $\mathbb{K}$-Vektorräume mit $\dim(V), \dim(W) < \infty$ und $f \in \mathrm{Hom}(V,W)$, dann gilt $\dim(\ker(f)) + \dim(\mathrm{im}(f)) = \dim(V)$.

Beweis. Sei $f\colon V \to W$. Wir betrachten eine Basis von $\ker(f)$. Wir wählen einen Unterraum $U \subseteq V$, sodass U komplementär zu $\ker(f)$ ist, also $V = \ker(f) \dot{+} U$. Wir behaupten $f|_U\colon U \to \mathrm{im}(f)$ ist ein Isomorphismus. Dazu zeigen wir, dass $f|_U$ surjektiv und injektiv ist.

Sei $\boldsymbol{w} \in \mathrm{im}(f)$, sprich $\exists \boldsymbol{v} \in V\colon f(\boldsymbol{v}) = \boldsymbol{w}$. Wir suchen ein $\boldsymbol{u} \in U$, sodass $f(\boldsymbol{u}) = \boldsymbol{w}$. Wir wissen $V = \ker(f) \dot{+} U$, womit $\exists \boldsymbol{v}_0 \in \ker(f)\colon \exists \boldsymbol{u} \in U\colon \boldsymbol{v} = \boldsymbol{v}_0 + u$ und $\boldsymbol{w} = f(\boldsymbol{v}) = f(\boldsymbol{v}_0) + f(\boldsymbol{u}) = f(\boldsymbol{u})$.

Mit Satz 5.13 zeigen wir nur noch $\ker(f|_U) = \{0\}$. Sei $\boldsymbol{u} \in U$ mit $f|_U(\boldsymbol{u}) = 0$, d.h. $\boldsymbol{u} \in V$ und $f(\boldsymbol{u}) = 0$, womit $\boldsymbol{u} \in \ker(f) \Rightarrow \boldsymbol{u} \in U \cap \ker(f) = \{0\}$.

Damit ist $f|_U\colon U \to \mathrm{im}(f)$ bijektiv, womit $\dim(U) = \dim(\mathrm{im}(f))$ und damit ist $\dim(\ker(f)) + \dim(U) = \dim(\ker(f)) + \dim(\mathrm{im}(f))$. □

Satz 5.15: Homomorphiesatz

Seien V, W $\mathbb{K}$-Vektorräume mit $f \in \mathrm{Hom}(V,W)$. Sei $\tilde{f}\colon V/\ker(f) \to \mathrm{im}(f)$ mit $[\boldsymbol{v}] \mapsto f(\boldsymbol{v})$, dann ist $\tilde{f}$ ein Isomorphismus.

Beweis. Wir prüfen, ob $\tilde{f}$ wohldefiniert ist, sprich $\tilde{f}$ ist vom Repräsentanten unabhängig. Seien $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$ mit $[\boldsymbol{v}_1] = [\boldsymbol{v}_2]$, dann gilt $\boldsymbol{v}_1 - \boldsymbol{v}_2 \in \ker(f)$:

$$\tilde{f}([\boldsymbol{v}_2]) = f(\boldsymbol{v}_2) + 0 = f(\boldsymbol{v}_2) + f(\boldsymbol{v}_1 - \boldsymbol{v}_2) = f(\boldsymbol{v}_2 + \boldsymbol{v}_1 - \boldsymbol{v}_2) = f(\boldsymbol{v}_1) = \tilde{f}([\boldsymbol{v}_1])$$

Wir prüfen weiterhin, ob $\tilde{f}$ linear ist. Seien $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$ und $\lambda, \mu \in \mathbb{K}$:

$$\tilde{f}(\lambda[\boldsymbol{v}_1] + \mu[\boldsymbol{v}_2]) = \tilde{f}([\lambda\boldsymbol{v}_1 + \mu\boldsymbol{v}_2]) = f(\lambda\boldsymbol{v}_1 + \mu\boldsymbol{v}_2) = \lambda f(\boldsymbol{v}_1) + \mu f(\boldsymbol{v}_2) = \lambda\tilde{f}([\boldsymbol{v}_1]) + \mu\tilde{f}([\boldsymbol{v}_2])$$

Da $\mathrm{im}(\tilde{f}) = \{\tilde{f}([\boldsymbol{v}]) | \boldsymbol{v} \in V\} = \{f(\boldsymbol{v}) | \boldsymbol{v} \in V\} = \mathrm{im}(f)$ behaupten wir, dass $\tilde{f}$ surjektiv ist. Sei $\boldsymbol{w} \in \mathrm{im}(f)$, dann gilt $\exists \boldsymbol{v} \in V\colon f(\boldsymbol{v}) = \boldsymbol{w} = \tilde{f}([\boldsymbol{v}])$. $\tilde{f}$ ist surjektiv. Es verbleibt die Injektivität. Seien $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V/\ker(f)$ mit $\tilde{f}([\boldsymbol{v}_1]) = \tilde{f}([\boldsymbol{v}_2])$:

$$\tilde{f}([\boldsymbol{v}_1]) - \tilde{f}([\boldsymbol{v}_2]) = 0 \Leftrightarrow f(\boldsymbol{v}_1 - \boldsymbol{v}_2) = 0 \Rightarrow \boldsymbol{v}_1 - \boldsymbol{v}_2 \in \ker(f)$$
$$[\boldsymbol{v}_2] = [\boldsymbol{v}_2] + [0] = [\boldsymbol{v}_2] + [\boldsymbol{v}_1 - \boldsymbol{v}_2] = [\boldsymbol{v}_2 + \boldsymbol{v}_1 - \boldsymbol{v}_2] = [\boldsymbol{v}_1]$$

Somit ist $\tilde{f}$ linear und bijektiv, womit $\tilde{f}$ ein Isomorphismus ist, wodurch $V/\ker(f) \simeq \mathrm{im}(f)$ beziehungsweise $\dim(V/\ker(f)) = \dim(\mathrm{im}(f))$. □

Da nach Satz 4.14 $\dim(V/\ker(f)) = \dim(V) - \dim(\ker(f))$ ist die Aussage des Homomorphiesatzes äquivalent zu Satz 5.14.

Seien $\dim(V) = \dim(W)$ und $f \in \mathrm{Hom}(V, W)$, dann sind die folgenden Aussagen äquivalent:

i f ist ein Monomorphismus

ii f ist ein Epimorphismus

iii f ist ein Isomorphismus

6 Matrizenrechnung

Wir haben bereits den Vektorraum $\mathrm{Hom}(V,W)$ untersucht, wobei $f_{ij}\colon \boldsymbol{v}_k \mapsto \delta_{kf}\boldsymbol{w}_i$. Wir haben Matrizen bereits im Zusammenhang mit linearen Gleichungssystemen gesehen. Wir werden sehen, dass $f \in \mathrm{Hom}(V,W)$ eine Darstellung mittels $f = \sum_{i,j} \alpha_{ij} f_{ij}$ hat. Dabei bilden die α_{ij} die Koeffizienten eines linearen Gleichungssystems.

Definition 6.1: Matrix

Eine Matrix über einem Körper $\mathbb{K}$ ist ein Zahlenschema:

$$\mathrm{A} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

mit m Zeilen und n Spalten. Die Menge $M_{m,n}(\mathbb{K})$ oder $\mathbb{K}^{m\times n}$ ist die Menge aller $m \times n$ Matrizen. $M_n(\mathbb{K}) = \mathbb{K}^{n\times n}$. Wir nennen $\boldsymbol{z}_i = (a_{i1}, a_{i2}, \dots, a_{in})$ den i-ten Zeilenvektor und:

$$\boldsymbol{s}_j = \begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix}$$

den j-ten Spaltenvektor. Die Hauptdiagonale $\mathrm{diag}(\mathrm{A}) = (a_{11}, a_{22}, \dots, a_{kk})$ wobei $k = \min(m,n)$. Wenn $m = n$ und $a_{ij} = 0$ für $i \neq j$, nennen wir A Diagonalmatrix:

$$\mathrm{A} = \begin{bmatrix} a_{11} & 0 & \dots & \dots & 0 \\ 0 & a_{22} & 0 & \dots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \dots & 0 & a_{nn} \end{bmatrix} \qquad \mathrm{I}_n = \begin{bmatrix} 1 & 0 & \dots & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \dots & 0 & 1 \end{bmatrix} = (\delta_{ij})_{ij=1,\dots,n}$$

Wir nennen I_n die Einheitsmatrix.

$$\mathrm{O} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & a_{nn} \end{bmatrix} \qquad \mathrm{U} = \begin{bmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & a_{22} & \ddots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$$

Wir nennen U eine untere Dreiecksmatrix und O eine obere Dreiecksmatrix. Die Matrix $(\mathrm{E}_{ij})_{kl} = [\delta_{jk}\delta_{jl}]$. Eine Matrix E_{ij} heißt (i,j)-Elementarmatrix. Die zu einer gegebenen Matrix $\mathrm{A} \in \mathbb{K}^{m\times n}$ transponierte Matrix $\mathrm{A}^T \in \mathbb{K}^{n\times m}$ mit Einträgen $(\mathrm{A}^T)_{ij} = a_{ji}$. Das Transponieren entspricht einer Spiegelung an der Hauptdiagonale. Dabei gilt $(\mathrm{A}^T)^T = \mathrm{A}$.

Wir werden Zeilenvektoren der Dimension n mit $1\times n$ Matrizen identifizieren und Spaltenvektoren der Dimension m mit $m \times 1$ Matrizen.

Satz 6.1

$\mathbb{K}^{m\times n}$ mit den Operationen $[a_{ij}]_{m\times n} + [b_{ij}]_{m\times n} = [a_{ij} + b_{ij}]_{m\times n}$ und $\lambda[a_{ij}]_{m\times n} = [\lambda a_{ij}]_{m\times n}$ ist ein Vektorraum mit Basis $(\mathrm{E}_{ij})_{\substack{i=1,\dots,m \\ j=1,\dots,n}}$ und $\dim(\mathbb{K}^{m\times n}) = mn$.

Beispiel:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = a\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + b\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + c\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + d\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = a\mathrm{E}_{11} + b\mathrm{E}_{12} + c\mathrm{E}_{21} + d\mathrm{E}_{22}$$

Es sei angemerkt, dass $\mathbb{K}^{m\times n} \to \mathbb{K}^{n\times m}$ mit $\mathrm{A} \mapsto \mathrm{A}^T$ ist ein Isomorphismus.

Definition 6.2: Matrizenmultiplikation

Sei $\mathrm{A} = [a_{ij}]_{\substack{i=1,\dots,m\\ j=1,\dots,n}} \in \mathbb{K}^{m\times n}$ und $\boldsymbol{x} = (x_1, \dots, x_n) \in \mathbb{K}^n$. Dann heißt der Vektor:

$$\mathrm{A}\boldsymbol{x} = \begin{bmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^n a_{1j}x_j \\ \sum_{j=1}^n a_{2j}x_j \\ \vdots \\ \sum_{j=1}^n a_{mj}x_j \end{bmatrix} = \left[\sum_{j=1}^n a_{ij}x_j\right]_{m\times 1} \in \mathbb{K}^m$$

Wir können nun ein Lineares Gleichungssystem als $\mathrm{A}\boldsymbol{x} = \boldsymbol{b}$ anschreiben. Dabei sind $\boldsymbol{x}$ die Unbekannten Größen, A die Koeffizienten und $\boldsymbol{b}$ die Konstanten.

Beispiel:

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \begin{bmatrix} 7 \\ 8 \\ 9 \end{bmatrix} = \begin{bmatrix} 7 + 16 + 27 \\ 28 + 40 + 54 \end{bmatrix}$$

Es sei angemerkt, dass $\mathrm{A}\boldsymbol{e}_k = \boldsymbol{s}_k(\mathrm{A})$ (die k-te Spalte) ergibt.

Satz 6.2

Sei $\mathrm{A} \in \mathbb{K}^{m\times n}$:

i die Abbildung $f_{\mathrm{A}} \colon \mathbb{K}^n \to \mathbb{K}^m$ mit $\boldsymbol{x} \mapsto \mathrm{A}\boldsymbol{x}$ linear

ii $\forall f \in \mathrm{Hom}(\mathbb{K}^n, \mathbb{K}^m) \colon \exists! \mathrm{A} \in \mathbb{K}^{m\times n} \colon f = f_{\mathrm{A}}$

iii $\mathcal{M} \colon \mathbb{K}^{m\times n} \to \mathrm{Hom}(\mathbb{K}^n, \mathbb{K}^m)$ mit $\mathrm{A} \mapsto f_{\mathrm{A}}$ ist ein Isomorphismus

Beweis. Zu (i)

Seien $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{K}^n$ und $\lambda, \mu \in \mathbb{K}$. Sei weiters $\mathrm{A} \in \mathbb{K}^{m\times n}$. Wir zeigen $\mathrm{A}(\lambda\boldsymbol{v} + \mu\boldsymbol{w}) = \lambda\mathrm{A}\boldsymbol{v} + \mu\mathrm{A}\boldsymbol{w}$. Nach Satz 6.1 ist $\lambda[a_{ij}]_{m\times n} = [\lambda a_{ij}]_{m\times n}$. Mit Definition 6.2 erhalten wir somit:

$$\begin{aligned} \mathrm{A}(\lambda\boldsymbol{v} + \mu\boldsymbol{w}) &= \mathrm{A}\left(\lambda\,[v_j]_{1\times n} + \mu\,[w_j]_{1\times n}\right) = \mathrm{A}\left([\lambda v_j + \mu w_j]_{1\times n}\right) \\ &= \left[\sum_{j=1}^n a_{ij}(\lambda v_j + \mu w_j)\right]_{m\times 1} = \left[\sum_{j=1}^n \lambda a_{ij}v_j + \sum_{j=1}^n \mu a_{ij}w_j\right]_{m\times 1} \\ &= \lambda\left[\sum_{j=1}^n a_{ij}v_j\right]_{m\times 1} + \mu\left[\sum_{j=1}^n a_{ij}w_j\right]_{m\times 1} = \lambda\mathrm{A}\boldsymbol{v} + \mu\mathrm{A}\boldsymbol{w} \end{aligned}$$

Zu (ii)

Wir wissen aus Satz 5.10, dass zwei lineare Abbildungen $f, g \in \mathrm{Hom}(V, W)$ gleich sind, wenn die Bilder der Basis von V gleich sind. Insbesondere können wir eine lineare Abbildung $f \in \mathrm{Hom}(V, W)$ durch das Bild der Basis von V eindeutig vorgeben. Wir betrachten die Basis der kanonischen Basisvektoren $(\boldsymbol{e}_1, \dots, \boldsymbol{e}_n)$ des $\mathbb{K}^n$. Sei $f \in \mathrm{Hom}(\mathbb{K}^n, \mathbb{K}^m)$ eine lineare Funktion. Wir wissen, dass f eindeutig durch $f((\boldsymbol{e}_1, \dots, \boldsymbol{e}_n))$ vorgegeben wird. Mit Definition 6.2 erhalten wir:

$$\mathrm{A}\boldsymbol{e}_i = \boldsymbol{s}_i(\mathrm{A})$$

Insbesondere soll gelten $\forall i \in \{1, \dots, n\} \colon \mathrm{A}\boldsymbol{e}_i = f(\boldsymbol{e}_i)$. Wir wählen daher:

$$\mathrm{A} = [f(\boldsymbol{e}_i)]_{1\times n} = [\mathrm{E}_{ij} f(\boldsymbol{e}_i)_j]_{m\times n} \Rightarrow \forall i \in \{1, \dots, n\} \colon \mathrm{A}\boldsymbol{e}_i = f(\boldsymbol{e}_i)$$

Da f eindeutig ist, ist auch f_{A}, und somit A, eindeutig.

Zu (iii)

Sei $f \in \mathrm{Hom}(\mathbb{K}^n, \mathbb{K}^m)$, dann können wir nach (ii) eine Matrix A finden, sodass $f_A = f$. Somit ist $\mathcal{M}$ surjektiv. Da diese Matrix A eindeutig bestimmt ist, ist auch f eindeutig bestimmt, womit gilt $A_1 = A_2 \Rightarrow \gamma(A_1) = \gamma(A_2)$. Somit ist $\mathcal{M}$ bijektiv. Es verbleibt zu zeigen, dass $\mathcal{M}$ linear ist. Seien $A_1, A_2 \in \mathbb{K}^{m\times n}$ und $\lambda \in \mathbb{K}$. Wir wissen bereits $\lambda A = [\lambda a_{ij}]_{m\times n}$, womit für $\boldsymbol{v} \in \mathbb{K}^m$ gilt $f_{\lambda A}(\boldsymbol{v}) = \lambda A\boldsymbol{v} = \lambda f_A(\boldsymbol{v})$. Zur Additivität:

$$f_{A_1+A_2}(\boldsymbol{v}) = (A_1 + A_2)\boldsymbol{v} = [a_{1,ij} + a_{2,ij}]_{m\times n}\,\boldsymbol{v} = \left[\sum_{j=1}^{n} a_{1,ij}v_j + \sum_{j=1}^{n} a_{2,ij}v_j\right]_{m\times 1}$$

$$= \left[\sum_{j=1}^{n} a_{1,ij}v_j\right]_{m\times 1} + \left[\sum_{j=1}^{n} a_{2,ij}v_j\right]_{m\times 1} = A_1\boldsymbol{v} + A_2\boldsymbol{v}$$

Somit ist $\mathcal{M}$ linear, womit $\mathbb{K}^{m\times n} \simeq \mathrm{Hom}(\mathbb{K}^n, \mathbb{K}^m)$. □

Wir wollen uns nun damit beschäftigen, zwei lineare Abbildungen A und B hintereinander auszuführen, also $f_A \circ f_B = A(B\boldsymbol{x}) = (AB)\boldsymbol{x}$? Wir benötigen also ein allgemeines Matrix-Produkt.

Definition 6.3: Verallgemeinertes Matrix Produkt

Seien $A \in \mathbb{K}^{n\times m}$ und $B \in \mathbb{K}^{m\times p}$, dann heißt die Matrix $C = AB \in \mathbb{K}^{n\times p}$ das Produkt von A und B und hat die folgenden Einträge:

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

Mit anderen Worten: $\boldsymbol{s}_j(C) = A\boldsymbol{s}_j(B)$.

Beispiel:

$$\begin{bmatrix}1 & 2 & 3\\ 4 & 5 & 6\end{bmatrix}\begin{bmatrix}1 & 2\\ 3 & 4\\ 5 & 6\end{bmatrix} = \begin{bmatrix}1+6+15 & 2+8+18\\ 4+15+30 & 8+20+36\end{bmatrix} = \begin{bmatrix}22 & 28\\ 49 & 64\end{bmatrix}$$

Beispiel:

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

Im Allgemeinen ist das Matrix-Produkt nicht kommutativ.

Satz 6.3

Seien A, B Matrizen, wobei $A \in \mathbb{K}^{n\times m}$ und $B \in \mathbb{K}^{m\times p}$, dann gilt $f_A \circ f_B = f_{AB}$, wobei $f_{AB} \colon \mathbb{K}^p \to \mathbb{K}^n$.

Beweis. Aufgrund Satz 5.10 genügt es zu zeigen, dass die Bilder der kanonischen Basis ident sind, also $\forall k \in \{1, \dots, p\} \colon (f_A \circ f_B)(\boldsymbol{e}_k) = f_{AB}(\boldsymbol{e}_k)$.

$$(f_A \circ f_B)(\boldsymbol{e}_k) = f_A(f_B(\boldsymbol{e}_k)) = Af_B(\boldsymbol{e}_k) = A\boldsymbol{s}_k(B) = \boldsymbol{s}_k(AB) = (AB)\boldsymbol{e}_k = f_{AB}(\boldsymbol{e}_k)$$

□

Korollar 6.1: Assoziativät des Matrix-Produktes

Seien A, B, C Matrizen, deren Produkt $A(BC)$ gebildet werden kann, dann gilt $A(BC) = (AB)C$.

Beweis. Aus dem Beweis von Satz 6.3 folgt:

$$f_{A(BC)} = f_A \circ (f_B \circ f_C) = (f_A \circ f_B) \circ f_C = f_{(AB)C}$$

□

Satz 6.4

Rechenregeln für Matrizen:

i $\forall A \in \mathbb{K}^{n\times m} : \forall B, C \in \mathbb{K}^{m\times p} : A(B+C) = AB + AC$

ii $\forall A, B \in \mathbb{K}^{n\times m} : \forall C \in \mathbb{K}^{m\times p} : (A+B)C = AC + BC$

iii $\forall \lambda \in \mathbb{K} : \forall A \in \mathbb{K}^{n\times m} : \forall B \in \mathbb{K}^{m\times p} : (\lambda A)B = \lambda(AB) = A(\lambda B)$

iv $\forall A \in \mathbb{K}^{m\times n} : AI_n = A$ und $\forall B \in \mathbb{K}^{n\times m} : I_n B = B$

v $\forall A \in \mathbb{K}^{n\times m} : \forall B \in \mathbb{K}^{m\times p} : (AB)^T = B^T A^T \in \mathbb{K}^{p\times n}$

Beweis. Zu i)

Seien $A \in \mathbb{K}^{n\times m}$ und $B, C \in \mathbb{K}^{m\times p}$:

$$A(B+C) = A\left[b_{ij} + c_{ij}\right]_{m\times p} = \left[\sum_{k=1}^{m} a_{ik}(b_{kj} + c_{kj})\right]_{n\times p}$$
$$= \left[\sum_{k=1}^{m} a_{ij}b_{kj}\right]_{n\times p} + \left[\sum_{k=1}^{m} a_{ik}c_{kj}\right]_{n\times p} = AB + AB$$

ii) geht analog zu i)

Zu iii)

Sei $\lambda \in \mathbb{K}$ und $A \in \mathbb{K}^{n\times m}$ und $B \in \mathbb{K}^{m\times p}$:

$$(\lambda A)B = [\lambda a_{ij}]_{n\times m} B = \left[\sum_{k=1}^{m} \lambda a_{ik}b_{kj}\right]_{n\times p} = \left[\lambda \sum_{k=1}^{m} a_{ik}b_{kj}\right]_{n\times p} = \lambda(AB)$$
$$\left[\sum_{k=1}^{m} \lambda a_{ik}b_{kj}\right]_{n\times p} = \left[\sum_{k=1}^{m} a_{ik}(\lambda b_{kj})\right]_{n\times p} = A(\lambda B)$$

Zu iv)

Seien $A \in \mathbb{K}^{m\times n}$ und $B \in \mathbb{K}^{n\times m}$:

$$AI_n = [A\boldsymbol{s}_j(I_n)]_{1\times n} = [A\boldsymbol{e}_j]_{1\times n} = [\boldsymbol{s}_j(A)]_{1\times n} = A$$
$$I_n B = [I_n \boldsymbol{s}_j(B)]_{1\times m} = [\boldsymbol{s}_j(B)]_{1\times m} = B$$

Das Produkt $I_n B$ gilt, da $\forall \boldsymbol{v} \in \mathbb{K}^n : I_n \boldsymbol{v} = \boldsymbol{v}$, da $f_{I_n} = \mathrm{id} \in \mathrm{End}(\mathbb{K}^n)$.

Zu v) Seien $A \in \mathbb{K}^{n\times m}$ und $B \in \mathbb{K}^{m\times p}$:

$$((AB)^T)_{ij} = (AB)_{ji} = \sum_{k=1}^{m} a_{jk}b_{ki}$$
$$= \sum_{k=1}^{m} (A^T)_{kj}(B^T)_{ik} = \sum_{k=1}^{m} (B^T)_{ik}(A^T)_{kj} = (B^T A^T)_{ij}$$

□

Korollar 6.2

$(\mathbb{K}^{n\times n}, \cdot, +, \cdot_K)$, wobei $\cdot_K$ die Skalarmultiplikation ist und $\cdot$ die Matrizenmultiplikation, ist eine nichtkommutative Algebra über $\mathbb{K}$.
$(\mathbb{K}^{n\times n}, \cdot)$ ist ein Monoid mit neutralen Element I_n.

Definition 6.4: Inverse Matrix

Eine Matrix $A \in \mathbb{K}^{n\times n}$ heißt regulär bzw. invertierbar, wenn $\exists B \in \mathbb{K}^{n\times n}$: $AB = BA = I_n$. Wenn A nicht regulär ist, ist A singulär.

Satz 6.5: Eindeutigkeit der Inversen

Eine Matrix A hat höchstens eine Inverse, die, sofern existent, mit A^{-1} bezeichnet wird.

Beweis. Angenommen B, B' sind invers zu A:

$$B = BI = B(AB') = (BA)B' = IB' = B'$$

□

Satz 6.6

i I_n ist regulär
ii $A, B \in \mathbb{K}^{n\times n}$ sind regulär, dann ist (AB) regulär und $(AB)^{-1} = B^{-1}A^{-1}$
iii $A \in \mathbb{K}^{n\times n}$ ist regulär, dann ist A^{-1} regulär und $(A^{-1})^{-1} = A$
iv $A \in \mathbb{K}^{n\times n}$ ist regulär, dann ist A^T regulär und $(A^T)^{-1} = (A^{-1})^T$
v A ist regulär, wenn $f_A : \mathbb{K}^n \rightarrowtail \mathbb{K}^n$ und es gilt $f_A^{-1} = f_{A^{-1}}$

Beweis. Da $(\mathbb{K}^{n\times n}, \cdot)$ ein Monoid ist, sind i) bis iii) bereits bewiesen. Wir betrachten nun iv). Wir suchen also eine Matrix $B \in \mathbb{K}^{n\times n}$, sodass $A^TB = BA^T = I_n$. Wir behaupten nun, dass $B = (A^{-1})^T$:

$$A^T(A^{-1})^T = (A^{-1}A)^T = I_n$$
$$(A^{-1})^TA^T = (AA^{-1})^T = I_n$$

Zu v) Wir zeigen $f_A \circ f_B = \mathrm{id}$. Wir wissen bereits $f_A \circ f_B = f_{AB}$ und $\mathrm{id} = f_{I_n}$, sprich $AB = I_n$. □

Beispiele: Eine triviale reguläre Matrix ist die Einheitsmatrix I_n, da $I_nI_n = I_n$. Etwas interessanter ist etwa: Sei $A \in \mathbb{K}^{n\times n}$ regulär, dann ist für $\lambda \in \mathbb{K}$ $(\lambda A)^{-1} = \frac{1}{\lambda}A^{-1}$. Seien $a_{ii} \in \mathbb{K} \setminus \{0\}$, dann ist $\mathrm{diag}(a_{ii})$ invers zu $\mathrm{diag}(\frac{1}{a_{ii}})$.

Sei $\sigma \in S_n$ eine Permutation, dann ist $f_\sigma : \mathbb{K}^n \to \mathbb{K}^n$ mit $\boldsymbol{e}_i \mapsto \boldsymbol{e}_{\sigma(i)}$, dann ist $f_\sigma(\boldsymbol{v}) = A\boldsymbol{v}$ wobei $\boldsymbol{s}_i(A) = f_\sigma(\boldsymbol{e}_i) = \boldsymbol{e}_{\sigma(i)}$, sprich $A = [\boldsymbol{e}_{\sigma(i)}]_{1\times n}$. In jeder Spalte und Zeile kommt jeweils ein Einser vor, ansonsten sind alle $a_{ij} = 0$, dann nennen wir A eine *Permutationsmatrix*. Dann ist $f_\sigma^{-1} = f_{\sigma^{-1}}$, da σ bijektiv ist. Wir behaupten nun, dass für eine Permutationsmatrix A gilt $A^{-1} = A^T$:

$$(AA^T)_{ij} = \sum_{k=1}^{n} a_{ik}(A^T)_{kj} = \sum_{k=1}^{n} a_{ik}a_{jk}$$

Da $a_{ik}a_{jk} = 0$ für $i \neq j$ und für $i = j$: $a_{ik}a_{jk} = 1$ gilt:

$$(AA^T)_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases} \Rightarrow AA^T = I_n$$

Wir können auch geometrische Transformationen in $\mathbb{R}^2$ als lineare Abbildung beschreiben. Beginnen wir mit einer Rotation um einen Winkel α. Dabei erhalten wir den rechten Winkel zwischen $\boldsymbol{e}_1$ und $\boldsymbol{e}_2$. Die zugehörige Rotationsmatrix R_α hat dabei die Form:

$$\mathrm{R}_\alpha = \begin{bmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{bmatrix}$$

Aufgrund der Additionstheoreme[7] der Winkelfunktionen gilt:

$$\mathrm{R}_{\alpha+\beta} = \mathrm{R}_\alpha \mathrm{R}_\beta$$

Die inverse Matrix R_α^{-1} ist gegeben durch:

$$\mathrm{R}_\alpha^{-1} = \mathrm{R}_{-\alpha} = \begin{bmatrix} \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \cos(\alpha) \end{bmatrix} = \mathrm{R}_\alpha^T$$

Die Spiegelung entlang einer Geraden g S_α, wobei die Gerade g einen Winkel α zu $\boldsymbol{e}_1$ einschlägt, wird folgendermaßen ausgedrückt:

$$\mathrm{S}_\alpha = \begin{bmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{bmatrix}$$

Um zu zeigen, dass der Ausdruck stimmt betrachten wir zuerst eine Matrix S zur Spiegelung entlang der horizontalen Achse:

$$\mathrm{S} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Führen wir nun SR_α aus, so erhalten wir genau S_α. Ein Beispiel für eine singuläre Matrix ist etwa:

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

Angenommen $\mathrm{BA} = \mathrm{I}_2$, dann muss aber gelten:

$$\boldsymbol{e}_2 = (\mathrm{BA})\boldsymbol{e}_2 = \mathrm{B}(\mathrm{A}\boldsymbol{e}_2) = \mathrm{B}0 = 0$$

Definition 6.5: General Linear Group

$\mathrm{GL}(n, \mathbb{K}) = \{\mathrm{A} \in \mathbb{K}^{n\times n} | \exists \mathrm{A}^{-1} \in \mathbb{K}^{n\times n} \colon \mathrm{A}\mathrm{A}^{-1} = \mathrm{I}_n\}$. Dabei steht GL für General Linear Group.

Definition 6.6

i zwei Matrizen $\mathrm{A}, \mathrm{B} \in \mathbb{K}^{m\times n}$ heißen äquivalent, wenn $\exists \mathrm{P} \in \mathrm{GL}(m, \mathbb{K}) \colon \exists \mathrm{Q} \in \mathrm{GL}(n, \mathbb{K}) \colon \mathrm{A} = \mathrm{PBQ}$
ii zwei Matrizen $\mathrm{A}, \mathrm{B} \in \mathbb{K}^{n\times n}$ heißen ähnlich, wenn $\exists \mathrm{P} \in \mathrm{GL}(n, \mathbb{K}) \colon \mathrm{A} = \mathrm{P}^{-1}\mathrm{BP}$

Satz 6.7

i Äquivalenz ist eine Äquivalenzrelation auf $\mathbb{K}^{m\times n}$
ii Ähnlichkeit ist eine Äquivalenzrelation auf $\mathbb{K}^{n\times n}$

Beweis. Zu i)

$$\mathrm{A} = \mathrm{PAQ} \Rightarrow \mathrm{P} = \mathrm{I}_m, \mathrm{Q} = \mathrm{I}_n$$

Wir sehen direkt, dass die Äquivalenz reflexiv ist. Da P, Q regulär sind, gilt:

$$\mathrm{A} = \mathrm{PBQ} \Leftrightarrow \mathrm{P}^{-1}\mathrm{AQ}^{-1} = \mathrm{B}$$

[7] siehe Analysis 1

Somit ist die Äquivalenz auch symmetrisch. Als letztes prüfen wir auf Transitivität:

$$\mathrm{A} \sim \mathrm{B} \wedge \mathrm{B} \sim \mathrm{C} \Leftrightarrow \mathrm{A} = \mathrm{PBQ} \quad \wedge \quad \mathrm{B} = \mathrm{KCL}$$
$$\Rightarrow \mathrm{A} = \mathrm{PKCLQ} \Leftrightarrow \mathrm{A} \sim \mathrm{C}$$

Somit ist die Äquivalenz transitiv und eine Äquivalenzrelation.

Zu ii)

$$\mathrm{A} = \mathrm{P}^{-1}\mathrm{AP} \Rightarrow \mathrm{P} = \mathrm{P}^{-1} = \mathrm{I}_n$$

Die Ähnlichkeit ist also reflexiv. Da P regulär ist, gilt weiter:

$$\mathrm{A} = \mathrm{P}^{-1}\mathrm{BP} \Leftrightarrow \mathrm{PAP}^{-1} = \mathrm{B}$$

Somit ist die Ähnlichkeit ebenfalls symmetrisch. Zuletzt prüfen wir auf Transitivität:

$$\mathrm{A} \sim \mathrm{B} \wedge \mathrm{B} \sim \mathrm{C} \Leftrightarrow \mathrm{A} = \mathrm{P}^{-1}\mathrm{BP} \quad \wedge \quad \mathrm{B} = \mathrm{Q}^{-1}\mathrm{CQ}$$
$$\Rightarrow \mathrm{A} = \mathrm{P}^{-1}\mathrm{Q}^{-1}\mathrm{CQP} \Leftrightarrow \mathrm{A} \sim \mathrm{C}$$

Somit ist die Ähnlichkeit transitiv und eine Äquivalenzrelation. □

Wir haben bereits gesehen, wenn $\exists \boldsymbol{v} \neq 0$: $\mathrm{A}\boldsymbol{v} = 0$, dann ist A singulär, d.h. der Kern der Matrix $\mathrm{A} \neq \{0\}$, sprich $\dim(\ker(\mathrm{A})) > 0$ bzw. $\dim(\mathrm{im}(\mathrm{A})) < n$.

Definition 6.7: Bildraum

Sei $\mathrm{A} \in \mathbb{K}^{m \times n}$:

i $L(\boldsymbol{z}_1(\mathrm{A}), \ldots, \boldsymbol{z}_m(\mathrm{A})) \subseteq \mathbb{K}^n$ heißt Zeilenraum von A, dessen Dimension heißt Zeilenrang von A: $\mathrm{zrg}(\mathrm{A})$

ii $L(\boldsymbol{s}_1(\mathrm{A}), \ldots, \boldsymbol{s}_n(\mathrm{A})) \subseteq \mathbb{K}^m$ heißt der Spaltenraum von A, dessen Dimension heißt Spaltenrang von A: $\mathrm{srg}(\mathrm{A})$

Es sei angemerkt, dass aufgrund Satz 5.8 der Spaltenraum von $\mathrm{A} = \mathrm{im}(f_{\mathrm{A}})$. Weiters gilt $\mathrm{zrg}(\mathrm{A}) = \mathrm{srg}(\mathrm{A}^T)$.

Satz 6.8: Rang

Für $\mathrm{A} \in \mathbb{K}^{m \times n}$ ist $\mathrm{zrg}(\mathrm{A}) = \mathrm{srg}(\mathrm{A}) = \mathrm{rg}(\mathrm{A})$ der Rang von A.

Beweis. Es genügt zu zeigen, dass $\mathrm{srg}(\mathrm{A}) \leq \mathrm{zrg}(\mathrm{A})$, womit $\mathrm{srg}(\mathrm{A}^T) \leq \mathrm{zrg}(\mathrm{A}^T) \Leftrightarrow \mathrm{zrg}(\mathrm{A}) \leq \mathrm{srg}(\mathrm{A})$.

Sei $r = \mathrm{zrg}(\mathrm{A})$, das heißt der Zeilenraum hat Dimension r und wird durch $(\boldsymbol{z}_1(\mathrm{A}), \ldots, \boldsymbol{z}_m(\mathrm{A}))$ aufgespannt. Wir wählen aus diesen Zeilenvektoren eine Basis $(\boldsymbol{z}_{i_1}, \ldots, \boldsymbol{z}_{i_r})$, somit:

$$\exists \beta_{ij} \in \mathbb{K}\colon \boldsymbol{z}_k = \sum_{j=1}^{r} \beta_{kj} \boldsymbol{z}_{i_j}$$
$$1 \leq i \leq m \qquad 1 \leq j \leq r$$

Dann gilt:

$$\boldsymbol{z}_k = (a_{k1}, a_{k2}, \ldots, a_{kn})$$
$$\Rightarrow a_{kj} = (\boldsymbol{z}_k)_j = \sum_{l=1}^{r} \beta_{kl} (\boldsymbol{z}_{i_l})_j = \sum_{l=1}^{r} \beta_{kl} a_{i_l j}$$
$$\Rightarrow \boldsymbol{s}_j(\mathrm{A}) = \begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix} = \underbrace{\begin{bmatrix} \beta_{11} & \beta_{12} & \ldots & \beta_{1r} \\ \beta_{21} & \beta_{22} & \ldots & \beta_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{m1} & \beta_{m2} & \ldots & \beta_{mr} \end{bmatrix}}_{=\beta} \begin{bmatrix} a_{i_1 j} \\ a_{i_2 j} \\ \vdots \\ a_{i_r j} \end{bmatrix}$$

Das bedeutet, dass $\boldsymbol{s}_j(\mathrm{A})$ im Spaltenraum der Matrix β enthalten sind. Somit ist $L(\boldsymbol{s}_1(\mathrm{A}), \ldots, \boldsymbol{s}_n(\mathrm{A})) \subseteq L(\boldsymbol{s}_1(\beta), \ldots, \boldsymbol{s}_r(\beta))$, weshalb aber $\mathrm{srg}(\mathrm{A}) = \dim(L(\boldsymbol{s}_1(\mathrm{A}), \ldots, \boldsymbol{s}_n(\mathrm{A}))) \leq r = \mathrm{zrg}(\mathrm{A})$ gelten muss. □

Unser Ziel ist es nun, den Rang $\mathrm{rg}(A)$ zu bestimmen. Dabei ist die Berechnung des Ranges einer Diagonalmatrix trivial:

$$\mathrm{rg}(A) = |\{i \colon a_{ii} \neq 0\}|$$

Für allgemeine Matrizen werden wir Umformungen durchführen, um sie in die Form einer Diagonalmatrix zu bringen, ohne dabei den Rang der Matrix zu verändern.

Definition 6.8: Elementare Zeilenumformungen

Diese Umformungen sind gegeben durch:
- i Addition einer Zeile zu einer anderen, $\boldsymbol{z}_i \mapsto \boldsymbol{z}_i + \boldsymbol{z}_j$
- ii Multiplikation einer Zeile mit $\lambda \in \mathbb{K} \setminus \{0\}$, $\boldsymbol{z}_i \mapsto \lambda \boldsymbol{z}_i$

Analog sind die Spaltenumformungen definiert.

Wir sehen hier schon, dass diese Umformungen reversibel sind, sprich die zugehörigen Abbildungen sind bijektiv.

Satz 6.9: Weitere Umformungen

Auch die folgenden Umformungen lassen sich durch Kombination elementarer Umformungen erreichen:
- iii Vertauschen von zwei Zeilen
- iv Addition des λ-fachen einer Zeile zu einer anderen

Diese Umformungen können analog für Spalten erreicht werden.

Auch diese Komposita von Umformungen sind reversibel.

Beweis. Wir führen den Beweis für Spalten:

$$[\boldsymbol{s}_i, \boldsymbol{s}_j] \underset{(i)}{\mapsto} [\boldsymbol{s}_i, \boldsymbol{s}_i + \boldsymbol{s}_j] \underset{(ii)}{\mapsto} [-\boldsymbol{s}_i, \boldsymbol{s}_i + \boldsymbol{s}_j] \underset{(i)}{\mapsto} [\boldsymbol{s}_j, \boldsymbol{s}_i + \boldsymbol{s}_j] \underset{(ii)}{\mapsto} [-\boldsymbol{s}_j, \boldsymbol{s}_i + \boldsymbol{s}_j]$$
$$\underset{(i)}{\mapsto} [-\boldsymbol{s}_j, \boldsymbol{s}_i] \underset{(ii)}{\mapsto} [\boldsymbol{s}_j, \boldsymbol{s}_i]$$

So können wir eine Umformung vom Typ iii durchführen. Für Typ iv:

$$[\boldsymbol{s}_i, \boldsymbol{s}_j] \underset{(ii)}{\mapsto} [\boldsymbol{s}_i, \lambda \boldsymbol{s}_j] \underset{(i)}{\mapsto} [\boldsymbol{s}_i + \lambda \boldsymbol{s}_j, \lambda \boldsymbol{s}_j] \underset{(ii)}{\mapsto} [\boldsymbol{s}_i + \lambda \boldsymbol{s}_j, \boldsymbol{s}_j]$$

□

Satz 6.10

Jede Matrix $A \in \mathbb{K}^{m \times n}$ lässt sich durch eine Folge von Zeilen- und Spaltenumformungen i-iv auf die Gestalt:

$$\mathrm{I}_{mn}^{(r)} = \begin{bmatrix} \mathrm{I}_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$$

bringen. Dabei ist $I_{nm}^{(r)} \in \mathbb{K}^{m \times n}$.

Beweis. Wir wenden einen rekursiven Algorithmus an. Wenn $A = \mathbf{0}$, dann gilt $A = \mathrm{I}_{mn}^{(0)}$. Wenn in A mindestens ein Eintrag $a_{ij} \neq 0$, dann vertauschen wir die erste mit der i-ten Zeile und anschließend die erste mit der j-ten Spalte, sprich o.B.d.A $a_{11} \neq 0$. Schließlich dividieren wir die ersten Zeile durch a_{11} und erhalten somit die Form:

$$\begin{bmatrix} 1 & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & \dots & a_{mn} \end{bmatrix}$$

Mit Umformungen vom Typ iv erhalten wir weiters:

$$\begin{bmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathrm{A}_1 \end{bmatrix}$$

Wobei, $\mathrm{A}_1 \in \mathbb{K}^{(m-1)\times(n-1)}$. Wir wenden nun den gleichen Algorithmus auf A_1 an. Da $m, n \in \mathbb{N}$ stoppt dieser Algorithmus, wenn entweder $\mathrm{A}_k = \mathbf{0}$ oder aber wir haben alle Zeilen bzw. Spalten abgearbeitet. □

Wir werden sehen, dass $r = \mathrm{rg}(\mathrm{A})$, also der Rang invariant in Bezug auf Umformungen ist. Weiters kann eine Matrix nur mit Zeilenumformungen lediglich auf die Form einer oberen Dreiecksmatrix gebracht werden. Analog kann man nur mit Spaltenumformungen eine Matrix lediglich in die Form einer unteren Dreiecksmatrix bringen.

Satz 6.11

Sei $\mathrm{A} \in \mathbb{K}^{m\times n}$. Die folgenden Matrizen sind invertierbar und implementieren Zeilen- und Spaltenumformungen, durch Multiplikation von links (Zeilen) bzw. von rechts (Spalten):

i $\mathrm{T} = \mathrm{I} + \mathrm{E}_{ij}$

ii $\mathrm{T} = \mathrm{I} + (\lambda - 1)\mathrm{E}_{ii}$

iii $\mathrm{T} = \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 0 & 1 & & \\ & & 1 & 0 & & \\ & & & & \ddots & \\ & & & & & 1 \end{bmatrix}$

iv $\mathrm{T} = \mathrm{I} + \lambda \mathrm{E}_{ij}$

Beweis. Zu i. Sei $i \neq j$:

$$(\mathrm{I} + \mathrm{E}_{ij})(\mathrm{I} - \mathrm{E}_{ij}) = \mathrm{I} - \mathrm{E}_{ij} + \mathrm{E}_{ij} - \mathrm{E}_{ij}\mathrm{E}_{ij}$$

$$(\mathrm{E}_{ij}\mathrm{E}_{ij})_{kl} = \sum_{p=1}^{k} (\mathrm{E}_{ij})_{kp}(\mathrm{E}_{ij})_{pl} = \sum_{p=1}^{n} \delta_{kj}\delta_{jl}\delta_{ip}\delta_{jl} = \delta_{ik}\delta_{ij}\delta_{pl} = 0$$

$$\Rightarrow (\mathrm{I} + \mathrm{E}_{ij})(\mathrm{I} - \mathrm{E}_{ij}) = \mathrm{I}$$

Zu ii.

$$\mathrm{T}^{-1} = \mathrm{I} + \left(\frac{1}{\lambda} - 1\right)\mathrm{E}_{ij}$$

□

Satz 6.12

Jede Matrix ist äquivalent zu einer Matrix der Form $\mathrm{I}_{mn}^{(r)}$, d.h. $\exists \mathrm{P} \in \mathrm{GL}(m, \mathbb{K}), \mathrm{Q} \in \mathrm{GL}(n, \mathbb{K})$, sodass $\mathrm{A} = \mathrm{P}\mathrm{I}_{mn}^{(r)}\mathrm{Q}$.

Beweis. Es gibt elementare Zeilen- und Spaltenumformungen $\mathrm{L}_1 \dots \mathrm{L}_k \mathrm{A} \mathrm{R}_1 \dots \mathrm{R}_l = I_{mn}^{(r)}$. Dann können wir P und Q bestimmen: $\mathrm{P} = \mathrm{L}_1 \dots \mathrm{L}_k \in \mathrm{GL}(m, \mathbb{K})$ und $\mathrm{Q} = \mathrm{R}_1 \dots \mathrm{R}_l \in \mathrm{GL}(n, \mathbb{K})$. □

Lemma 6.1

Sei $\mathrm{A} \in \mathbb{K}^{m\times k}$ und $B \in \mathbb{K}^{k\times n}$, $\mathrm{rg}(\mathrm{AB}) \leq \min(\mathrm{rg}(\mathrm{A}), \mathrm{rg}(\mathrm{B}))$

Beweis.

$$\mathrm{rg}(\mathrm{AB}) = \mathrm{srg}(\mathrm{AB}) = \dim(\mathrm{im}(f_{\mathrm{AB}})) = \dim(\mathrm{im}(f_{\mathrm{A}} \circ f_{\mathrm{B}})) \leq \dim(\mathrm{im}(f_{\mathrm{A}})) = \mathrm{rg}(\mathrm{A})$$

$$\mathrm{rg}(\mathrm{AB}) = \mathrm{zrg}(\mathrm{AB}) = \mathrm{srg}((\mathrm{AB})^T) = \mathrm{srg}(\mathrm{B}^T\mathrm{A}^T) = \mathrm{rg}(\mathrm{B}^T\mathrm{A}^T) \leq \mathrm{rg}(\mathrm{B}^T) = \mathrm{rg}(\mathrm{B})$$

□

Satz 6.13

Äquivalente Matrizen haben den gleichen Rang. Sei $A \in \mathbb{K}^{m\times n}$, $P \in \mathbb{K}^{m\times m}$, $Q \in \mathbb{K}^{n\times n}$, dann gilt $\mathrm{rg}(PAQ) = \mathrm{rg}(A)$.

Beweis. Sei $A' = PA \Rightarrow \mathrm{rg}(A') \leq \mathrm{rg}(A)$. Und $P^{-1}A' = P^{-1}PA = A \Rightarrow \mathrm{rg}(A) \leq \mathrm{rg}(A')$, womit $\mathrm{rg}(A) = \mathrm{rg}(A')$. Analog gilt $\mathrm{rg}(AQ) = \mathrm{rg}(A)$. □

Korollar 6.3

Elementare Zeilen- und Spaltenumformungen ändern den Rang nicht.

Korollar 6.4

Am Ende der Umformungen in der Prozedur aus Satz 6.10 bleibt immer die gleiche Anzahl an Einsen übrig, nämlich $r = \mathrm{rg}(A)$.

Satz 6.14

Zwei Matrizen $A, B \in \mathbb{K}^{m\times n}$ sind äquivalent, wenn $\mathrm{rg}(A) = \mathrm{rg}(B)$.

Beweis. Mit Satz 6.13 verbleibt zu zeigen, dass $\mathrm{rg}(A) = \mathrm{rg}(B) \Rightarrow \exists P \in \mathrm{GL}(m,\mathbb{K}), Q \in \mathrm{GL}(n,\mathbb{K})\colon PAQ = B$.
Sei $\mathrm{rg}(A) = \mathrm{rg}(B) = r$. Es gilt:

$$\begin{aligned}&\exists P \in \mathrm{GL}(m,\mathbb{K}), Q \in \mathrm{GL}(n,\mathbb{K})\colon PAQ = I_{mn}^{(r)}\\ &\exists \tilde{P} \in \mathrm{GL}(m,\mathbb{K}), \tilde{Q} \in \mathrm{GL}(n,\mathbb{K})\colon \tilde{P}B\tilde{Q} = I_{mn}^{(r)}\\ &\Rightarrow PAQ = \tilde{P}B\tilde{Q} \Leftrightarrow \tilde{P}^{-1}PAQ = B\tilde{Q} \Leftrightarrow \tilde{P}^{-1}PAQ\tilde{Q}^{-1} = B\end{aligned}$$

Da $\tilde{P}^{-1}P \in \mathrm{GL}(m,\mathbb{K})$ und $Q\tilde{Q} \in \mathrm{GL}(n,\mathbb{K})$, sind A und B äquivalent. □

Satz 6.15

Eine Matrix $A \in \mathbb{K}^{n\times n}$ ist regulär, wenn $\mathrm{rg}(A) = n$. Man sagt auch, dass A vollen Rang hat.

Beweis. $\Rightarrow$, wenn A regulär ist, dann ist $A^{-1}A = I = I_{nn}^{(n)}$, womit $\mathrm{rg}(I) = n = \mathrm{rg}(A)$, da A äquivalent zu I_n.
$\Leftarrow$ $\mathrm{rg}(A) = n = \mathrm{rg}(I_n)$, dann ist A äquivalent zu I_n, womit:

$$\begin{aligned}&\exists P, Q \in \mathrm{GL}(n,\mathbb{K})\colon PAQ = I_n\\ &\Rightarrow A = P^{-1}I_nQ^{-1} = P^{-1}Q^{-1} \in \mathrm{GL}(n,\mathbb{K})\end{aligned}$$

□

Korollar 6.5

Jede reguläre Matrix kann als Produkt von elementaren Transformationsmatrizen geschrieben werden.

Beweis. Da A regulär ist, gilt $\mathrm{rg}(A) = \mathrm{rg}(I_n)$, womit:

$$L_k \dots L_1 A R_1 \dots R_l = I_n \Leftrightarrow A = L_1^{-1} \dots L_k^{-1} R_l^{-1} \dots R_1^{-1}$$

□

Korollar 6.6

Jede reguläre Matrix A lässt sich durch Zeilenumformungen allein in die Einheitsmatrix überführen.

Beweis. $A \in GL(n, \mathbb{K}) \Rightarrow A^{-1} \in GL(n, \mathbb{K})$:

$$A^{-1} = S_k \dots S_1$$

Dabei sind $S_1, \dots, S_k$ Transformationsmatrizen. Es gilt:

$$I_n = A^{-1}A = S_k \dots S_1 A$$

Da wir nur links multiplizieren, handelt es sich um Zeilenumformungen. □

Wir erhalten nun einen Algorithmus zur Bestimmung der Inversen. Wir wenden so lange Zeilenumformungen auf die Matrix A an, bis I_n herauskommt, dann produzieren die gleichen Zeilenumformungen angewandt auf die Einheitsmatrix die gesuchte inverse Matrix A^{-1}. Durch diesen Algorithmus kann man auch feststellen, ob eine gegebene Matrix A invertierbar ist. Kommt man nur mit Zeilenumformungen nicht auf die Einheitsmatrix, so ist A singulär. Dabei entspricht dieses Verfahren einer parallelen Anwendung des Gauß-Algorithmus mit den Einheitsvektoren $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$.

Lemma 6.2

Sei $A \in \mathbb{K}^{m \times k}$ und $B \in \mathbb{K}^{k \times n}$, dann ist $\operatorname{im}(AB) \subseteq \operatorname{im}(A)$. Wenn B regulär ist, dann ist $\operatorname{im}(AB) = \operatorname{im}(A)$. Analog ist $\operatorname{im}((AB)^T) \subseteq \operatorname{im}(B^T)$. Ist A regulär, so gilt Gleichheit.

Beweis. Wir wissen $\operatorname{im}(AB) \subseteq A$. Wenn B regulär ist, dann:

$$\operatorname{im}(A) = \operatorname{im}(ABB^{-1}) \subseteq \operatorname{im}(AB)$$

□

Korollar 6.7

i Elementare Spaltenumformungen ändern den Spaltenraum nicht
ii Elementare Zeilenumformungen ändern den Zeilenraum nicht

Wir erhalten nun eine Methode um eine Basis des Spaltenraums einer Matrix A zu bestimmen. Wir bringen A durch Spaltenumformungen allein auf Dreiecksgestalt, und entferne alle Nullspalten. Wir wenden also Gauß-Elimination auf die Spalten an (alternativ können wir auch Zeilenumformungen auf die transponierte Matrix anwenden).

6.1 Lineare Gleichungssysteme

Das lineare Gleichungssystem:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n &= b_2 \\ \vdots \qquad\qquad\qquad\qquad &\quad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n &= b_m \end{aligned}$$

kann als $A\boldsymbol{x} = \boldsymbol{b}$ geschrieben werden, wobei $A \in \mathbb{K}^{m \times n}$, und $\boldsymbol{x}, \boldsymbol{b}$ sind $m \times 1$ Spaltenvektoren. Wenn A regulär ist, dann ist $\boldsymbol{x} = A^{-1}\boldsymbol{b}$ die eindeutige Lösung. Wenn $\boldsymbol{b} = \boldsymbol{0}$, dann heißt das System *homogen*. Die Lösungsmenge des Systems $A\boldsymbol{x} = \boldsymbol{0}$ ist $\ker(A)$.

Satz 6.16: Lösbarkeit von Linearen Gleichungssystemen

Es sind äquivalent:
1. $A\boldsymbol{x} = \boldsymbol{b}$ ist lösbar
2. $\boldsymbol{b} \in \operatorname{im}(A)$
3. $\operatorname{rg}(A) = \operatorname{rg}(A|\boldsymbol{b})$

Beweis. $A\boldsymbol{x} = \boldsymbol{b}$ ist lösbar, ist äquivalent zu $\exists \boldsymbol{x} \in \mathbb{K}^n \colon f_A(x) = \boldsymbol{b} \Leftrightarrow b \in \operatorname{im}(f_A) \Leftrightarrow \boldsymbol{b} \in L(\boldsymbol{s}_i(A), \dots, \boldsymbol{s}_n(A)) \Leftrightarrow L(\boldsymbol{s}_1(A), \dots, \boldsymbol{s}_n(A)) = L(\boldsymbol{s}_1(A), \dots, \boldsymbol{s}_n(A), \boldsymbol{b}) \Leftrightarrow \dim(L(\boldsymbol{s}_1(A), \dots, \boldsymbol{s}_n(A))) = \dim(L(\boldsymbol{s}_1 A, \dots, \boldsymbol{s}_n(A), \boldsymbol{b})) \Leftrightarrow \operatorname{rg}(A) = \operatorname{rg}(A|\boldsymbol{b})$ □

In der Praxis ist dieses Kriterium nicht sonderlich nützlich, da es auf die zweifache Anwendung der Gauß-Elimination hinausläuft, um die Ränge zu bestimmen. Es ist weniger aufwendig, mit einer Gauß-Elimination das System zu lösen. Eine (im allgemeinen falsche) Faustegel ist, bei m Gleichungen mit n Unbekannten gibt es $n - m$ freie Parameter.

Satz 6.17

1. $A \in \mathbb{K}^{m \times n}$, dann bildet die Lösungsmenge L des homogenen Systems $A\boldsymbol{x} = \boldsymbol{0}$ einen Unterraum $L = \ker(A)$ mit $\dim(L) = n - \operatorname{rg}(A)$
2. Für jeden Unterraum $U \subseteq \mathbb{K}^n$ mit $\dim(U) = r$, gilt: $\forall m \geq n - r \colon \exists A \in \mathbb{K}^{m \times n} \colon U = \ker(A)$
3. Für $\boldsymbol{b} \in \mathbb{K}^m$ sei $\boldsymbol{x}_0 \in \mathbb{K}^n$ eine beliebige Lösung des Systems $A\boldsymbol{x} = \boldsymbol{b}$, dann ist die Lösungsmenge L die lineare Mannigfaltigkeit $L = \boldsymbol{x}_0 + \ker(A)$

Beweis.
1. $\dim(\ker(A)) + \dim(\operatorname{im}(A)) = n$ und $\dim(L) + \operatorname{rg}(A) = n$
2. Ü
3. Angenommen $A\boldsymbol{x}_0 = \boldsymbol{b}$, dann $A\boldsymbol{x}_0 - A\boldsymbol{x} = \boldsymbol{b} - \boldsymbol{b} = \boldsymbol{0}$ somit $A(\boldsymbol{x}_0 - \boldsymbol{x}) = \boldsymbol{0}$ womit $\boldsymbol{x}_0 - \boldsymbol{x} \in \ker(A) \Leftrightarrow \boldsymbol{x} \in \boldsymbol{0} + \ker(A)$

□

Einige Bemerkungen zur Gauß-Jordan Elimination:

1. Elementare Zeilenumformungen entsprechen Multiplikation mit regulären Matrizen von links:
   - Zeilenvertauschung T_{ij} ist eine Permutationsmatrix und vertauscht $\boldsymbol{z}_i$ mit $\boldsymbol{z}_j$
   - Addition der k-ten Zeile zu einer anderen.
2. L ist eine reguläre Matrix, dann ist $A\boldsymbol{x} = \boldsymbol{b} \Leftrightarrow LA\boldsymbol{x} = L\boldsymbol{b}$ d.h. elementare Zeilenumformungen ändern die Lösungsmenge nicht
3. $Q \in \mathbb{K}^{n \times n}$, regulär, $AQ\boldsymbol{x} = \boldsymbol{b}$ ändert die Lösungsmenge, aber $AQ\boldsymbol{y} = \boldsymbol{b}$, dann $\boldsymbol{x} = Q\boldsymbol{y}$ bzw. $\boldsymbol{y} = Q^{-1}\boldsymbol{x}$
4. Wenn $A \in \mathbb{K}^{n \times n}$ regulär ist, Zeilenumformungen $(A|I_n) \to (I_n|A_n)$ was der simultanen Lösung der Gleichungssysteme $A\boldsymbol{x} = \boldsymbol{e}_i$, wobei $A\boldsymbol{s}_i(A^{-1}) = \boldsymbol{e}_i$

Satz 6.18: Gauß-Jordan Elimination

Sei $A \in \mathbb{K}^{m \times n}$, dann $\exists P \in \mathbb{K}^{m \times m}$ Permutationsmatrix und $L \in \mathbb{K}^{m \times m}$ eine reguläre untere Dreiecksmatrix und $R \in \mathbb{K}^{m \times n}$ eine obere Dreiecksmatrix, sodass $PA = LR$. Dann ist $A\boldsymbol{x} = \boldsymbol{b} \Leftrightarrow P^{-1}LR\boldsymbol{x} = \boldsymbol{b} \Leftrightarrow LR\boldsymbol{x} = P\boldsymbol{b} \Leftrightarrow R\boldsymbol{x} = L^{-1}P\boldsymbol{b}$.

Lemma 6.3: Frobenius-Matrizen

Die Matrizen der Form

$$\mathcal{F}_k^{n\times n} = \left\{ \begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & 1 & \ddots & \vdots \\ \vdots & & \lambda_{k+1} & \ddots & 0 \\ 0 & \cdots & \lambda_n & 0 & 1 \end{bmatrix}, \lambda_i \in \mathbb{K} \right\} = \left\{ \mathrm{I}_n + \sum_{i=k+1}^{n} \lambda_i \mathrm{E}_{ik} | \lambda_i \in \mathbb{K} \right\}$$

heißen ***Frobenius-Matrizen*** und bilden eine Gruppe bezüglich Multiplikation.

Beweis für Lemma 6.3.

$$\begin{aligned} &\left(\mathrm{I}_n + \sum_{i=k+1}^{n} \lambda_i \mathrm{E}_{ik}\right)\left(\mathrm{I} + \sum_{j=k+1}^{n} \mu_j \mathrm{E}_{jk}\right) \\ &= \mathrm{I}_n + \sum_{i=k+1}^{n} \lambda_i \mathrm{E}_{ik} + \sum_{j=k+1}^{n} \mu_j \mathrm{E}_{jk} + \sum_{i,j=k+1}^{n} \lambda_i \mu_j \mathrm{E}_{ik}\mathrm{E}_{jk} \\ &= \mathrm{I}_n + \sum_{i=k+1}^{n} (\lambda_i + \mu_i)\mathrm{E}_{ik} \overset{!}{=} \mathrm{I}_n \Rightarrow \mu_i = -\lambda_i \\ &\Rightarrow \left(\mathrm{I}_n + \sum_{i=k+1}^{n} \lambda_i \mathrm{E}_{ik}\right)^{-1} = \mathrm{I}_n - \sum_{i=k+1}^{n} \lambda_i \mathrm{E}_{ik} \end{aligned}$$

□

Erörtern wir nun einen Algorithmus induktiv. Wir beginnen mit $\mathrm{A}^{(0)} = \mathrm{A}$. Wir suchen nun die erste Spalte $\boldsymbol{s}_{j_1}(\mathrm{A}) \neq \mathbf{0}$. Wir finden dann den größten Eintrag $a_{i_1 j_1}$ und vertauschen dann die i_1-te Zeile mit der ersten Zeile. Danach erzeugen wir mit einer Frobenius-Matrix $\mathrm{F}_1 \in \mathcal{F}_1$ in der j_1 Spalte Nullen unter $a_{i_1 j_1}$. Wir kennen auch die Einträge λ_i:

$$\lambda_i = \begin{cases} -\frac{a_{ij_1}}{a_{i_1 j_1}} & i \neq i_1 \\ -\frac{a_{1 j_1}}{a_{i_1 j_1}} & i = i_1 \end{cases}$$

Dann hat $\mathrm{A}^{(1)} = \mathrm{F}_1 \mathrm{T}_{(1,i_1)} \mathrm{A}$ die Form:

$$\begin{bmatrix} 0 & \cdots & 0 & a_{i_1 j_1} & \cdots \\ \vdots & & \vdots & 0 & \\ \vdots & & \vdots & \vdots & \mathrm{B} \\ 0 & \cdots & 0 & 0 & \end{bmatrix}$$

Wir wenden nun diesen Algorithmus auf die Matrix B an. Wir erhalten dafür $\mathrm{F}_2 \in \mathcal{F}_2$ und $\mathrm{T}_{(2,i_2)}$ und erhalten somit $\mathrm{A}^{(2)} = \mathrm{F}_2 \mathrm{T}_{(2,i_2)} \mathrm{A}^{(1)}$. Am Ende erhalten wir ein Produkt aus Frobenius-Matrizen und Transpositionen:

$$\left(\prod_{k=\mathrm{rgA}}^{1} \mathrm{F}_k \mathrm{T}_{(k,i_k)}\right) \mathrm{A} = \mathrm{F}_{\mathrm{rgA}} \mathrm{T}_{(\mathrm{rgA}, i_{\mathrm{rgA}})} \cdots \mathrm{F}_1 \mathrm{T}_{(i_1,1)} \mathrm{A} = \mathrm{R}$$

Lemma 6.4: Erhalt von Frobenius-Matrizen unter Transpositionen

Sei $\mathrm{F} \in \mathcal{F}_k^{m\times m}$ eine Frobenius Matrix und T_π eine Permutationsmatrix mit $\pi(i) = i \forall i \leq k$, dann ist $\mathrm{T}_\pi \mathrm{F} \mathrm{T}_\pi^{-1} \in \mathcal{F}_k^{m\times m}$.

Somit folgt:

$$\begin{aligned} \mathrm{A} &= \mathrm{T}_{(i_1,1)} \mathrm{F}_1^{-1} \mathrm{T}_{(i_2,2)} \cdots \mathrm{F}_r^{-1} \mathrm{R} \\ &= \mathrm{P}^{-1} \mathrm{F}_1' \mathrm{F}_2' \cdots \mathrm{F}_r' \mathrm{R} = \mathrm{P}^{-1} \mathrm{L} \mathrm{R} \end{aligned}$$