Lineare Algebra

U. Stammbach

Professor an der ETH-Zürich

I. Vektorräume

I. Vektorräume

In diesem Kapitel führen wir den Leser zuerst in einen Problemkreis ein, in welchem später Methoden der linearen Algebra auf exemplarische Weise angewendet werden sollen. Es handelt sich dabei um lineare Gleichungssysteme. Resultate der linearen Algebra werden nicht nur zu grösserer Einsicht in diesen Problemkreis, sondern auch zu effizienten Lösungsmethoden führen. Wir zeigen anschliessend, wie sich einige grundlegende Konzepte der linearen Algebra, nämlich *Matrix*, *Linearkombination*, *Vektorraum* auf natürliche Weise an linearen Gleichungssystemen illustrieren lassen. Mit Hilfe eines Axiomensystems definieren wir dann den Begriff *Vektorraum über einem Körper* und zeigen an Beispielen, dass Vektorräume vielen dem Leser bereits bekannten mathematischen Strukturen zugrunde liegen. Das Kapitel schliesst mit einem kurzen Abschnitt über den algebraischen Begriff *Körper*. Dabei geht es *nicht* um eine systematische Behandlung, sondern es soll hier nur auf die Allgemeinheit der Definition eines Vektorraumes aufmerksam gemacht werden.

I.1. Lineare Gleichungssysteme

Wir betrachten in diesem Abschnitt reelle lineare Gleichungssyteme und stellen einige vorbereitende Bemerkungen über Matrizen zusammen.

1.1. Ein *reelles lineares Gleichungssystem* mit m Gleichungen in n Unbekannten $x_1, \ldots, x_n$ lässt sich in der folgenden Form schreiben:

$$\text{(B)} \quad \left| \begin{array}{ccc} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = & b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n & = & b_2 \\ \vdots & & \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n & = & b_m \end{array} \right|$$

Dabei bezeichnen a_{ik}, b_i für $1 \leq k \leq n$, $1 \leq i \leq m$ reelle Zahlen. Das System (B) heisst *homogen*, wenn $b_1 = b_2 = \cdots = b_m = 0$, andernfalls heisst es *inhomogen*. Das n-Tupel

$(\xi_1, \xi_2, \ldots, \xi_n)$ von reellen Zahlen heisst *Lösung* von (B), wenn alle Gleichungen von (B) durch Einsetzen von $\xi_1, \xi_2, \ldots, \xi_n$ anstelle von $x_1, \ldots, x_n$ befriedigt werden. Die Menge der Lösungen heisst *Lösungsmenge* von (B).

1.2. **Satz.** *Es sei* (H) *ein homogenes System in n Unbekannten, und es seien die n-Tupel* $(\xi_1, \xi_2, \ldots, \xi_n)$ *und* $(\eta_1, \eta_2, \ldots, \eta_n)$ *Lösungen von* (H)*. Dann ist auch das n-Tupel* $(\xi_1 + \eta_1, \xi_2 + \eta_2, \ldots, \xi_n + \eta_n)$ *eine Lösung von* (H)*, und für jede reelle Zahl λ ist auch* $(\lambda\xi_1, \lambda\xi_2, \ldots, \lambda\xi_n)$ *eine Lösung von* (H)*.*

Ein homogenes System besitzt insbesondere immer die triviale Lösung $(0, 0, \ldots, 0)$. Ist (B) ein beliebiges System, so bezeichne ($\mathrm{H_B}$) das *das zugehörige homogene System*, d.h. dasjenige System, das aus (B) entsteht, wenn anstelle von $b_1, b_2, \ldots, b_m$ jeweils 0 eingesetzt wird.

1.3. **Satz.** *Es sei* (B) *ein beliebiges System und* ($\mathrm{H_B}$) *das zugehörige homogene System. Ist* $(\zeta_1, \zeta_2, \ldots, \zeta_n)$ *eine Lösung von* (B) *und* $(\xi_1, \xi_2, \ldots, \xi_n)$ *eine Lösung von* ($\mathrm{H_B}$)*, dann ist* $(\zeta_1 + \xi_1, \zeta_2 + \xi_2, \ldots, \zeta_n + \xi_n)$ *eine Lösung von* (B)*.*

Man beweist die Sätze 1.2 und 1.3 durch einfaches Einsetzen. Die Einzelheiten überlassen wir dem Leser. Im Folgenden bezeichnen wir die n-Tupel wiederum mit Symbolen $\xi = (\xi_1, \xi_2, \ldots, \xi_n)$, $\eta = (\eta_1, \eta_2, \ldots, \eta_n)$, $\zeta = (\zeta_1, \zeta_2, \ldots, \zeta_n)$ und definieren eine Addition und eine Multiplikation mit einer reellen Zahl $\lambda \in \mathbb{R}$ wie folgt:

$$\begin{aligned} \xi + \eta &= (\xi_1 + \eta_1, \xi_2 + \eta_2, \ldots, \xi_n + \eta_n)\ , \\ \lambda\xi &= (\lambda\xi_1, \lambda\xi_2, \ldots, \lambda\xi_n)\ . \end{aligned}$$

1.4. Der Leser stellt sehr leicht fest, dass die Lösungsmenge des Systems (B) durch folgende Operationen nicht verändert wird:

(i) Vertauschen von Gleichungen,

(ii) Multiplikation einer Gleichung mit $\lambda \in \mathbb{R}$, $\lambda \neq 0$,

(iii) Addition des λ-fachen der j-ten Gleichung zur i-ten Gleichung; $i \neq j$.

Diese Feststellung kann dazu verwendet werden, ein gegebenes System schrittweise in ein einfacheres überzuführen, an dem die Lösungsmenge direkt abgelesen werden kann.

1.5. Beispiel.

$$\left|\begin{array}{ccccccccc} x & & & - & z & + & 3w & = & 0 \\ & & 4y & - & 4z & & & = & 0 \\ x & - & y & - & z & + & w & = & 0 \end{array}\right| \qquad \left|\begin{array}{ccccccccc} x & & & - & z & + & 3w & = & 0 \\ & & y & - & z & & & = & 0 \\ x & - & y & & - & z & +w & = & 0 \end{array}\right|$$

$$\left|\begin{array}{rrrrrrrrr} x & & & - & z & + & 3w & = & 0 \\ & & y & - & z & & & = & 0 \\ & - & y & & & - & 2w & = & 0 \end{array}\right| \qquad \left|\begin{array}{rrrrrrrr} x & & - & z & + & 3w & = & 0 \\ & y & - & z & & & = & 0 \\ & & & z & + & 2w & = & 0 \end{array}\right|$$

$$\left|\begin{array}{rrrrrrrr} x & & & & + & 5w & = & 0 \\ & y & - & z & & & = & 0 \\ & & & z & + & 2w & = & 0 \end{array}\right| \qquad \left|\begin{array}{rrrrrrr} x & & & + & 5w & = & 0 \\ & y & & + & 2w & = & 0 \\ & & z & + & 2w & = & 0 \end{array}\right| .$$

Am letzten Gleichungssystem lässt sich die Lösungsmenge direkt ablesen. Setzen wir nämlich $w = \lambda \in \mathbb{R}$, so ist $x = -5\lambda$, $y = -2\lambda$, $z = -2\lambda$. Die Lösungsmenge lässt sich also beschreiben durch

$$\{\xi = (\xi_1, \xi_2, \xi_3, \xi_4) \,|\, \xi_1 = -5\lambda, \xi_2 = -2\lambda, \xi_3 = -2\lambda, \xi_4 = \lambda,\ \lambda \in \mathbb{R}\} \ .$$

1.6. **Satz.** *Es sei* (H) *ein homogenes Gleichungssystem mit weniger Gleichungen als Unbekannte, d.h. $m < n$. Dann existiert immer eine nichttriviale Lösung, d.h. eine Lösung ξ, $\xi = (\xi_1, \xi_2, \ldots, \xi_n)$, die von der trivialen Lösung* $(0, 0, \ldots, 0)$ *verschieden ist.*

Beweis. Vollständige Induktion nach n. Induktionsverankerung: $m = 1$, $n = 2$. Für beliebige a und b besitzt die Gleichung $ax+by = 0$ eine nichttriviale Lösung. Induktionsschritt: Der Satz sei richtig für $n-1$ Unbekannte und $m < n-1$ Gleichungen. Sind im Gleichungssystem

$$\text{(H)} \qquad \left|\begin{array}{ccc} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = & 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n & = & 0 \\ \vdots & & \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n & = & 0 \end{array}\right| , \quad m < n \ ,$$

alle $a_{ik} = 0$, so ist jedes n-Tupel eine Lösung. Wir dürfen daher nach allfälliger Umnumerierung der Gleichungen und der Unbekannten $a_{11} \neq 0$ annehmen. Wenn wir für $i \geq 2$ zur i-ten Gleichung, das $(-a_{i1}/a_{11})$-fache der ersten addieren, so erhalten wir ein äquivalentes System

$$\left|\begin{array}{rcc} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = & 0 \\ a^*_{22}x_2 + \cdots + a^*_{2n}x_n & = & 0 \\ \vdots\qquad & & \vdots \\ a^*_{m2}x_2 + \cdots + a^*_{mn}x_n & = & 0 \end{array}\right|$$

Das Teilsystem

$$\left|\begin{array}{ccc} a^*_{22}x_2 + \cdots + a^*_{2n}x_n & = & 0 \\ \vdots & & \vdots \\ a^*_{m2}x_2 + \cdots + a^*_{mn}x_n & = & 0 \end{array}\right|$$

besitzt nach Induktionsvoraussetzung eine nichttriviale Lösung $(\xi_2, \ldots, \xi_n)$. Einsetzen in die erste Gleichung liefert einen Wert für ξ_1 so, dass $(\xi_1, \xi_2, \ldots, \xi_n)$ eine Lösung des ganzen Systems (H) ist. Damit ist Satz 1.6 bewiesen.

1.7. **Satz.** *Es sei* (B) *ein beliebiges System mit* $m = n$.

(i) *Besitzt* ($\mathrm{H_B}$) *nur die triviale Lösung, so besitzt* (B) *genau eine Lösung.*

(ii) *Besitzt* ($\mathrm{H_B}$) *eine nichttriviale Lösung, so besitzt* (B) *entweder keine oder unendlich viele Lösungen.*

Beweis. (i): Induktion nach n. Induktionsverankerung: Für $n = 1$ ist die Aussage sicher richtig. Induktionsschritt: Die Aussage (i) sei richtig für $n - 1$. Wir wollen beweisen, dass sie auch für n richtig ist. Da ($\mathrm{H_B}$) nur die triviale Lösung besitzt, ist mindestens eines der a_{ik} verschieden von Null. Wir dürfen daher nach allfälliger Umnumerierung $a_{11} \neq 0$ annehmen. Für $i \geq 2$ addieren wir zur i-ten Gleichung das $(-a_{i1}/a_{11})$-fache der ersten. Damit erhalten wir ein zu (B) äquivalentes Gleichungssystem:

$$\left| \begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = & b_1 \\ a_{22}^*x_2 + \cdots + a_{2n}^*x_n & = & b_2^* \\ \vdots \quad & & \vdots \\ a_{m2}^*x_2 + \cdots + a_{mn}^*x_n & = & b_m^* \end{array} \right| .$$

Das Teilsystem ($\mathrm{H_B^*}$) besitzt nur die triviale Lösung, sonst hätte ($\mathrm{H_B}$) eine nichttriviale Lösung. Nach Induktionsvoraussetzung besitzt deshalb das Teilsystem (B^*) genau *eine* Lösung, die wir mit $(\xi_2, \ldots, \xi_n)$ bezeichnen. Durch Einsetzten in die erste Gleichung erhalten wir auf eindeutige Weise ein ξ_1. Damit ist $(\xi_1, \xi_2, \ldots, \xi_n)$ *die* eindeutige Lösung von (B).

(ii): Ist η eine Lösung von (B) und ξ eine Lösung von ($\mathrm{H_B}$), so ist $\eta + \lambda\xi$ für beliebiges $\lambda \in \mathbb{R}$ wiederum eine Lösung von (B). In diesem Fall gibt es also unendlich viele Lösungen. Die einzige andere Möglichkeit ist, dass (B) *keine* Lösung besitzt.

1.8. Als Folgerung halten wir noch fest:

Ein inhomogenes System (B) mit gleichvielen Gleichungen wie Unbekannten besitzt entweder *eine eindeutig bestimmte Lösung* oder *das zugehörige homogene System* ($\mathrm{H_B}$) *besitzt eine nichttriviale Lösung.*

Wir werden in Abschnitt II.6 im allgemeinen Zusammenhang noch einmal auf lineare Gleichungssystem zurückkommen und dann in der Lage sein, die obigen Sätze besser zu erklären. Hier wollen wir noch einige Bemerkungen über Matrizen anfügen.

1.9. **Definition.** Eine reelle $m \times n$-Matrix ist ein rechteckiges Schema von reellen Zahlen

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{bmatrix} , \quad A = [a_{ik}] \ .$$

Der erste Index numeriert die *Zeilen*, der zweite die *Spalten* der Matrix. Das *Element* a_{ik} steht somit in der i-ten Zeile und in der k-ten Spalte. Wir definieren die *Summe* von zwei $m \times n$-Matrizen A und B durch

$$A + B = [a_{ik}] + [b_{ik}] = [a_{ik} + b_{ik}]$$

und das *Produkt* einer Matrix A mit einer Zahl $\lambda \in \mathbb{R}$ durch

$$\lambda[a_{ik}] = [\lambda a_{ik}] \ .$$

Ein n-Tupel kann als eine $1 \times n$-Matrix angesehen werden. Die für n-Tupel eingeführten Operationen, Summe und Produkt mit einer reellen Zahl, stimmen mit den für Matrizen definierten Operationen überein. Eine $n \times n$-Matrix heisst *quadratisch*. Die $n \times n$-Matrix I,

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} , \quad I = [\delta_{ik}] \ ,$$

heisst *Einheitsmatrix* der Ordnung n. Das sogenannte *Kronecker-Symbol* δ_{ik} ist definiert durch

$$\delta_{ik} = \begin{cases} 1 & \text{für } i = k \ , \\ 0 & \text{sonst} \ . \end{cases}$$

Eine quadratische Matrix $[a_{ik}]$ mit $a_{ik} = 0$ für $i \neq k$ heisst *Diagonalmatrix*. Die Elemente a_{ii} heissen *Diagonalelemente*.

Es sei A eine $m \times n$-Matrix und B eine $n \times p$-Matrix. In diesem Fall – und nur in diesem Fall – definieren wir ein *Produkt* $C = AB$. Die Matrix C ist eine $m \times p$-Matrix. Gilt $A = [a_{ij}]$, $B = [b_{jk}]$ und $C = [c_{ik}]$, so ist C definiert durch

$$c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk} = a_{i1} b_{1k} + a_{i2} b_{2k} + \cdots + a_{in} b_{nk} \ , \quad 1 \leq i \leq m \ , \quad 1 \leq k \leq p \ .$$

1.10. Beispiele.

$$\begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 4 & 5 \\ 6 & 7 \end{bmatrix} = \begin{bmatrix} 6 & 7 \\ 26 & 31 \end{bmatrix} ,$$

$$\begin{bmatrix} 4 & 5 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix} = \begin{bmatrix} 10 & 19 \\ 14 & 27 \end{bmatrix} ,$$

$$\begin{bmatrix} 0 & 1 & 2 \\ 3 & 4 & 5 \end{bmatrix} \begin{bmatrix} 6 & 7 \\ 8 & 9 \end{bmatrix} \text{ nicht definiert,}$$

$$\begin{bmatrix} 0 & 1 & 2 \\ 3 & 4 & 5 \end{bmatrix} \begin{bmatrix} 6 \\ 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 23 \\ 86 \end{bmatrix} .$$

Ist A eine $m \times n$-Matrix, und ist I die Einheitsmatrix der Ordnung m und I' die Einheitsmatrix der Ordnung n, so gilt $IA = A = AI'$.

1.11. Im Beispiel 1.10 haben wir festgestellt, dass die Matrizenprodukte AB und BA nicht immer existieren und dass sie, auch wenn beide definiert sind, verschieden sein können. Hingegen gelten die folgenden allgemeinen Rechenregeln:

$$\begin{array}{ccccc} A(B+C) & & = & & AB + AC \ , \\ (\lambda A)B & = & \lambda(AB) & = & A(\lambda B) \ , \\ A(BC) & & = & & (AB)C \ . \end{array}$$

Diese Regeln zu beweisen, überlassen wir dem Leser.

1.12. Zu einem linearen Gleichungssystem

$$\sum_{k=1}^{n} a_{ik} x_k = b_i \ , \quad 1 \le i \le m \ ,$$

gehören die *Koeffizientenmatrix* A und die *augmentierte Koeffizientenmatrix* A',

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} , \quad A' = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{bmatrix} .$$

Führt man die $m \times 1$-Matrix b und die $n \times 1$-Matrix x,

$$b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix} , \quad x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

ein, so kann das Gleichungssystem in der kompakten Form

$$Ax = b$$

geschrieben werden.

1.13. **Übungsaufgaben.**
1. Man führe die Beweise von Satz 1.2 und Satz 1.3 explizit durch.
2. Man beweise die in 1.11 aufgeführten Rechenregeln für die Matrizenmultiplikation.
3. Man betrachte das Gleichungssystem

$$\left| \begin{array}{ccccc} ax & + & b^2y & = & a-b \\ a^2x & + & by & = & b-a \end{array} \right|$$

und diskutiere die Lösungsmenge in den Fällen (i) $ab \neq 0$, (ii) $ab = 0$, (iii) $a = b$, (iv) $a + b = 0$.
4. Man beweise: Es sei (B) ein beliebiges inhomogenes Gleichungssystem, und es sei ζ eine feste Lösung von (B). Dann ist jede Lösung von (B) von der Form $\eta = \zeta + \xi$, wobei ξ eine Lösung des zugehörigen homogenen Systems ($\mathrm{H_B}$) ist.
5. Für die Matrizen A und B,

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

berechne man $A(AB)$ und $(AA)B$.
6. Gegeben seien die Matrizen C, I,

$$C = \begin{bmatrix} 3 & 1 \\ -1 & 4 \end{bmatrix} , \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} .$$

Gibt es eine Matrix D mit $DC = I$? Ist D eindeutig bestimmt? Berechne CD.

I.2. Beispiele von Vektorräumen

Im Abschnitt I.3 werden wir den Begriff *Vektorraum* axiomatisch definieren. Hier seien zunächst einige Beispiele von Vektorräumen aufgezählt, die dem Leser wohlbekannt sein dürften. Die Axiome, die in Abschnitt I.3 die Definition des Begriffes Vektorraum ausmachen, sind in diesen Beispielen einfache und bekannte Rechenregeln.

Die Vektoren im dreidimensionalen Anschauungsraum bilden unter den üblichen Rechenregeln bezüglich Addition von Vektoren und Multiplikation eines Vektors mit einer reellen Zahl einen Vektorraum E^3 über den reellen Zahlen $\mathbb{R}$.

Wird im dreidimensionalen Anschauungsraum ein Koordinatensystem eingeführt, so lässt sich jeder Vektor durch ein reelles Zahlentripel beschreiben. Der Addition von Vektoren entspricht die Addition von Zahlentripeln

$$(x, y, z) + (x', y', z') = (x + x', y + y', z + z') \ .$$

Der Multiplikation eines Vektors mit einer reellen Zahl entspricht die Multiplikation eines Zahlentripels mit einer reellen Zahl

$$\lambda(x, y, z) = (\lambda x, \lambda y, \lambda z) \ , \quad \lambda \in \mathbb{R} \ .$$

Mit diesen Rechenregeln bilden die reellen Zahlentripel einen Vektorraum $\mathbb{R}^3$ über den reellen Zahlen $\mathbb{R}$.

Die n-Tupel reeller Zahlen bilden unter der in I.1 eingeführten Addition und Multiplikation mit einer reellen Zahl einen Vektorraum $\mathbb{R}^n$ über den reellen Zahlen $\mathbb{R}$:

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n) \ ,$$

$$\lambda(x_1, x_2, \ldots, x_n) = (\lambda x_1, \lambda x_2, \ldots, \lambda x_n) \ , \quad \lambda \in \mathbb{R} \ .$$

Die n-Tupel komplexer Zahlen bilden unter der Addition und der Multiplikation mit einer komplexen Zahl einen Vektorraum $\mathbb{C}^n$ über den komplexen Zahlen $\mathbb{C}$.

Die n-Tupel rationaler Zahlen bilden unter der Addition und der Multiplikation mit einer rationalen Zahl einen Vektorraum $\mathbb{Q}^n$ über den rationalen Zahlen $\mathbb{Q}$.

Wir wollen noch erwähnen, dass an die Stelle von $\mathbb{R}$, $\mathbb{C}$ und $\mathbb{Q}$ in den letzten drei Beispielen ein beliebiger sogenannter *Körper* treten kann (siehe I.5). Dabei sei schon jetzt festgehalten, dass die ganzen Zahlen $\mathbb{Z}$ *keinen* Körper bilden.

I.3. Definition eines Vektorraumes

Bei der Beschäftigung mit Vektorräumen zeigt es sich, dass viele in konkreten Beispielen wichtige Eigenschaften in Tat und Wahrheit logische Folgerungen aus ganz wenigen grundlegenden Eigenschaften sind. Wie fast überall in der Mathematik geht man deshalb "axiomatisch" vor. Man definiert den "Begriff" des Vektoraumes dadurch, dass man gewisse grundlegende Eigenschaften ("Axiome") fordert und leitet dann daraus weitere, kompliziertere Eigenschaften rein logisch her. Diese Folgerungen müssen dann notgedrungen überall dort gelten, wo die Axiome erfüllt sind ("Modelle").

Im Folgenden geben wir eine axiomatische Definition des Begriffes *Vektorraum über dem Körper F*. Näheres über den Begriff *Körper* wird im Abschnitt I.5 und im Anhang zu finden sein. Der Leser setze vorläufig $F = \mathbb{R}$, $F = \mathbb{C}$ oder $F = \mathbb{Q}$.

3.1. **Definition.** Es sei F ein Körper. Ein *Vektorraum* V über dem Körper F ist eine nicht leere Menge von Elementen $\{\alpha, \beta, \gamma, \ldots\}$ ("Vektoren"), zusammen mit einer *Addition* "+" und einer *skalaren Multiplikation* " $\cdot$ " mit folgenden Eigenschaften:

(i) Die Addition "+" ordnet jedem Paar (α, β), α, $\beta \in V$, ein Element $\alpha + \beta \in V$ zu, so dass die folgenden Regeln erfüllt sind:

- (V1) $\alpha + \beta = \beta + \alpha$, $\alpha, \beta \in V$,
- (V2) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$, $\alpha, \beta, \gamma \in V$,
- (V3) es gibt ein eindeutig bestimmtes Element $0 \in V$ ("Nullelement") mit $\alpha + 0 = \alpha$ für alle $\alpha \in V$,
- (V4) zu jedem $\alpha \in V$ gibt es ein eindeutig bestimmtes $(-\alpha) \in V$ mit der Eigenschaft $\alpha + (-\alpha) = 0$.

(ii) Die skalare Multiplikation " $\cdot$ " von Elementen in F mit Elemente in V ordnet jedem Paar (a, α) mit $a \in F$ und $\alpha \in V$ ein Element $a\alpha \in V$ zu, so dass die folgenden Regeln erfüllt sind:

- (V5) $a \cdot (\alpha + \beta) = (a \cdot \alpha) + (a \cdot \beta)$, $a \in F$, $\alpha, \beta \in V$,
- (V6) $(a + b) \cdot \alpha = (a \cdot \alpha) + (b \cdot \alpha)$, $a, b \in F$, $\alpha \in V$,
- (V7) $(a\, b) \cdot \alpha = a \cdot (b \cdot \alpha)$, $a, b \in F$, $\alpha \in V$,
- (V8) $1 \cdot \alpha = \alpha$, $\alpha \in V$.

Wir bemerken, dass das Produkt $a \cdot \alpha$ der Einfachheit halber gewöhnlich $a\alpha$ geschrieben wird.

Man zeigt leicht, dass die in Abschnitt I.2 genannten Beispiele diese Axiome erfüllen. Im Folgenden geben wir eine Reihe weiterer Beispiele an. In jedem einzelnen Fall müssen dabei festgelegt werden: der Körper F, die Menge V, die Addition in V und die Multiplikation von Elementen aus V mit Elementen aus F. Den Nachweis, dass die obigen Axiome in diesen Beispielen erfüllt sind, überlassen wir dem Leser.

3.2. Es sei $F = \mathbb{R}$. Die Menge der Folgen reeller Zahlen $\{(a_1, a_2, \ldots) \mid a_i \in \mathbb{R}\}$, zusammen mit der Addition "+" , definiert durch

$$(a_1, a_2, \ldots) + (b_1, b_2, \ldots) = (a_1 + b_1, a_2 + b_2, \ldots) \ ,$$

und der skalaren Multiplikation

$$\lambda(a_1, a_2, \ldots) = (\lambda a_1, \lambda a_2, \ldots) \ , \quad \lambda \in \mathbb{R} \ ,$$

bilden einen Vektorraum $\mathbb{R}^\infty$ über $\mathbb{R}$. Die Untermengen der konvergenten Folgen bzw. der Nullfolgen, zusammen mit den oben definierten Operationen sind ebenfalls Vektorräume $\bar{\mathbb{R}}^\infty$, $\bar{\mathbb{R}}_0^\infty$ über $\mathbb{R}$.

3.3. Ein reelles Polynom $f(x)$ ist ein Ausdruck der Form

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \ ,$$

wobei x eine sogenannte Unbestimmte und $a_0, a_1, \ldots, a_n$ reelle Zahlen sind. Die Menge der reellen Polynome, zusammmen mit der üblichen Addition von Polynomen und der üblichen Multiplikation von Polynomen mit reellen Zahlen bildet einen Vektorraum $P_\infty(\mathbb{R})$ über $\mathbb{R}$. Ist n eine natürliche Zahl, so ist die Untermenge der reellen Polynome vom Grad kleiner oder gleich n, zusammen mit der üblichen Addition und der üblichen skalaren Multiplikation ein Vektorraum $P_n(\mathbb{R})$ über $\mathbb{R}$. Analog lassen sich Vektorräume $P_\infty(\mathbb{Q})$ und $P_n(\mathbb{Q})$ über $\mathbb{Q}$ definieren.

3.4. Es sei ein reelles homogenes lineares Gleichungssystem

$$\text{(H)} \qquad \sum_{k=1}^{n} a_{ik} x_k = 0 \ , \quad i = 1, \ldots, m \ ,$$

gegeben. Definiert man die Addition und die skalare Multiplikation von Lösungen von (H) wie in $\mathbb{R}^n$, so bilden die Lösungen von (H) einen Vektorraum über $\mathbb{R}$, den *Lösungsraum* von (H). (Der Leser mache sich klar, dass die analoge Aussage für ein *inhomogenes* System *nicht* richtig ist.)

3.5. Es sei $F = \mathbb{R}$ und V die Menge der n-Tupel komplexer Zahlen. Die Addition in V sei wie in $\mathbb{C}^n$ definiert und die Multiplikation von Elementen in $\mathbb{R}$ mit Elementen aus V durch

$$a(c_1, \ldots, c_n) = (ac_1, \ldots, ac_n) \ , \quad a \in \mathbb{R} \ , c_1, \ldots, c_n \in \mathbb{C} \ .$$

Damit wird V zu einem Vektorraum über $\mathbb{R}$.

3.6. Es sei V die Menge aller reellwertigen, auf dem Intervall $[0, 1]$ stetigen Funktionen. Für $f, g \in V$ und $a \in \mathbb{R}$ definieren wir

$$\begin{aligned} (f+g)(x) &= f(x) + g(x) \ , \quad x \in [0,1] \ , \\ (af)(x) &= a(f(x)) \ , \quad x \in [0,1] \ . \end{aligned}$$

Mit dieser Addition und skalaren Multiplikation wird V zu einem Vektorraum über $\mathbb{R}$, dem Vektorraum $C[0,1]$ der reellwertigen stetigen Funktionen auf dem Intervall $[0,1]$.

Es sei $c \in [0,1]$. Die Menge $\{f \in V \mid f(c) = 0\}$ zusammen mit den oben definierten Operationen ist ebenfalls ein Vektorraum über $\mathbb{R}$. Es ist klar, dass man in analoger Weise für jedes Intervall $[a,b]$ einen Vektorraum $C[a,b]$ definieren kann. Es ist auch klar, dass die Menge *aller* auf $[0,1]$ definierten reellwertigen Funktionen zusammen mit den oben beschriebenen Operationen ein Vektorraum über $\mathbb{R}$ ist.

Im folgenden Satz stellen wir einige einfache Folgerungen aus den Axiomen V1, ..., V8 zusammen.

3.7. **Satz.** *Es sei V ein Vektorraum über F. Für $\alpha, \beta \in V$ und $a \in F$ gelten die folgenden Aussagen:*

(i) $0 \cdot \alpha = 0$.

(ii) $a \cdot 0 = 0$.

(iii) *Aus $a \cdot \alpha = 0$ folgt $a = 0$ oder $\alpha = 0$.*

(iv) $(-a) \cdot \alpha = a \cdot (-\alpha) = -(a \cdot \alpha)$.

(v) *Es gilt $a \cdot (\alpha - \beta) = a \cdot \alpha - a \cdot \beta$ und $(a-b) \cdot \alpha = a \cdot \alpha - b \cdot \alpha$.*

Beweis. (i): Es gilt $0 \cdot \alpha = (0+0) \cdot \alpha = 0 \cdot \alpha + 0 \cdot \alpha$ nach V6. Nach V4 existiert zum Vektor β, $\beta = 0 \cdot \alpha$ ein Vektor $-\beta$ mit $0 \cdot \alpha + (-\beta) = 0$. Damit erhalten wir

$$\begin{aligned} 0 = 0 \cdot \alpha + (-\beta) &= (0 \cdot \alpha + 0 \cdot \alpha) + (-\beta) \\ &= 0 \cdot \alpha + (0 \cdot \alpha + (-\beta)) \quad \text{nach V2} \\ &= 0 \cdot \alpha + 0 \\ &= 0 \cdot \alpha \quad \text{nach V3.} \end{aligned}$$

(ii): Es gilt $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$ nach V5. Nach V4 existiert zum Vektor β, $\beta = a \cdot 0$ ein Vektor $-\beta$ mit $a \cdot 0 + (-\beta) = 0$. Damit folgt

$$\begin{aligned} 0 = a \cdot 0 + (-\beta) &= (a \cdot 0 + a \cdot 0) + (-\beta) \\ &= a \cdot 0 + (a \cdot 0 + (-\beta)) \quad \text{nach V2} \\ &= a \cdot 0 + 0 \\ &= a \cdot 0 \quad \text{nach V3 .} \end{aligned}$$

(iii): Es sei $a \cdot \alpha = 0$ und $a \neq 0$. Es ist zu zeigen, dass daraus $\alpha = 0$ folgt. Wegen $a \neq 0$ existiert $1/a$. Daraus folgt

$$\frac{1}{a}(a \cdot \alpha) = \frac{1}{a} \cdot 0 = 0$$

nach (ii). Andererseits gilt

$$\begin{aligned} \frac{1}{a}(a \cdot \alpha) &= \left(\frac{1}{a} \cdot a\right) \cdot \alpha \quad \text{nach V7} \\ &= 1 \cdot \alpha \\ &= \alpha \quad \text{nach V8.} \end{aligned}$$

Die Beweise der Aussagen (iv) und (v) überlassen wir dem Leser.

3.8. Wir bemerken ferner, dass nach dem assoziativen Gesetz V2 Klammern in einer Summe von mehreren Vektoren weggelassen werden dürfen und dass nach dem kommutativen Gesetz V1 die Reihenfolge der Summanden in einer Summe von mehreren Vektoren beliebig verändert werden darf. Wir überlassen die zwar nicht schwierigen, aber nur umständlich zu formulierenden Beweise für diese beiden Bemerkungen dem Leser und begnügen uns hier mit zwei Beispielen:

$$\begin{aligned} (\alpha + (\beta + \gamma)) + \delta &= ((\alpha + \beta) + \gamma) + \delta \\ &= (\alpha + \beta) + (\gamma + \delta) \\ &= \alpha + (\beta + (\gamma + \delta)) \ , \end{aligned}$$

$$\begin{aligned} \alpha + \beta + \gamma &= \alpha + \gamma + \beta \\ &= \beta + \gamma + \alpha \\ &= \beta + \alpha + \gamma \\ &= \gamma + \alpha + \beta \\ &= \gamma + \beta + \alpha \ . \end{aligned}$$

3.9. Um in der Folge die Notation etwas zu vereinfachen, führen wir das Summenzeichen auch für Vektoren ein. Wir definieren

$$\sum_{i=1}^{n} \alpha_i = \alpha_1 + \alpha_2 + \cdots + \alpha_n \ .$$

Es ist einfach zu sehen, dass dann die üblichen Rechenregeln gelten; für $a, a_1, \ldots, a_n$, $b_1, \ldots, b_n \in F$, $\alpha, \alpha_1, \ldots, \alpha_n \in V$ haben wir:

$$\text{(i)} \qquad a \cdot \sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} a \cdot \alpha_i \ ,$$

$$\text{(ii)} \qquad \left(\sum_{i=1}^{n} a_i\right) \cdot \alpha = \sum_{i=1}^{n} a_i \cdot \alpha \ ,$$

$$\text{(iii)} \qquad \sum_{i=1}^{n} a_i \cdot \alpha_i + \sum_{i=1}^{n} b_i \cdot \alpha_i = \sum_{i=1}^{n} (a_i + b_i) \cdot \alpha_i \ .$$

3.10. **Übungsaufgaben.**
1. Man beweise die Aussagen (iv) und (v) des Satzes 3.7.
2. Man beweise die Behauptungen 3.8 und 3.9.
3. Man löse das folgende lineare Gleichungssystem mit komplexen Koeffizienten:

$$\left| \begin{array}{ccccccc} 2x_1 & & & + & ix_3 & = & i \\ x_1 & - & 3x_2 & - & ix_3 & = & 2i \\ ix_1 & + & x_2 & + & x_3 & = & 1+i \end{array} \right| .$$

4. Man zeige, dass die reellen $m \times n$-Matrizen zusammen mit der üblichen Addition und skalaren Multiplikation einen Vektorraum über $\mathbb{R}$ bilden.
5. Es sei $W = \{f(x) \in P_\infty(\mathbb{R}) \,|\, f(x) = (-x)\}$. Ist W zusammen mit der üblichen Addition und skalaren Multiplikation ein Vektorraum über $\mathbb{R}$?
6. Man zeige, dass die reellwertigen, auf dem Intervall $(0,1)$ definierten und differenzierbaren Funktionen zusammen mit der üblichen Addition und skalaren Multiplikation einen Vektorraum über $\mathbb{R}$ bilden.
7. Man betrachte die Menge X der Paare reeller Zahlen und definiere die Addition durch $(x,y)+(x',y') = (x+x', y+y')$ und die Multiplikation mit einer reellen Zahl c durch $c(x,y) = (cx, y)$. Ist X zusammen mit diesen Operationen ein Vektorraum über $\mathbb{R}$?

I.4. Linearkombinationen, Unterräume

4.1. Als Beispiel betrachten wir zuerst den dreidimensionalen Anschauungsraum E^3. Es sei α ein Vektor in E^3, $\alpha \neq 0$. Fassen wir die Vielfachen $a\alpha$, $a \in \mathbb{R}$ als Ortsvektoren von Punkten auf, so bilden diese eine durch O gehende Gerade in Richtung α. Es seien α und β zwei nicht parallele Vektoren in E^3. Fassen wir erneut die Vektoren $a\alpha + b\beta$, $a, b \in \mathbb{R}$ als Ortsvektoren von Punkten auf, so bilden diese eine durch O gehende Ebene, die α und β enthält. Für Bildungen der Art $a\alpha$, $a\alpha + b\beta$, etc. hat man den Begriff *Linearkombination* eingeführt.

4.2. **Definition.** Es sei S eine (nicht leere) Familie von Vektoren des Vektorraumes V über F. Es sei

$$\alpha = \sum_{i=1}^{n} a_i \alpha_i \quad a_1, \ldots, a_n \in F \ , \quad \alpha_1, \ldots \alpha_n \in S \ .$$

Dann sagen wir, der Vektor $\alpha \in V$ sei als *Linearkombination* von Vektoren aus S dargestellt.

Die Menge der Vektoren, die sich als Linearkombinationen von Vektoren aus S darstellen lassen, bezeichen wir mit $[S]$ und nennen $[S]$ die *lineare Hülle* von S. Ist S endlich, $S = \{\alpha_1, \ldots, \alpha_p\}$, so schreiben wir auch $[\alpha_1, \ldots, \alpha_p]$ an Stelle von $[S]$ und sprechen statt von einer Linearkombination von Vektoren aus S auch etwa von einer Linearkombination der Vektoren $\alpha_1, \ldots, \alpha_p$.

4.3. Beispiel. Es sei V ein Vektorraum über F und $S = \{\alpha_1, \ldots, \alpha_p\}$. Dann ist $[S] = \{a_1\alpha_1 + \cdots + a_p\alpha_p \,|\, a_1, \ldots, a_p \in F\}$.

4.4. Beispiel. Es sei $V = \mathbb{R}^3$, $S = \{\epsilon_1, \epsilon_2, \epsilon_3\}$, $\epsilon_1 = (1,0,0)$, $\epsilon_2 = (0,1,0)$, $\epsilon_3 = (0,0,1)$. Dann ist $[S] = \mathbb{R}^3$.

4.5. Beispiel. Es sei $V = \mathbb{R}^3$, $S = \{(1,1,0), (1,0,1)\}$. Dann gilt

$$
\begin{aligned}
[S] &= \{(a(1,1,0) + b(1,0,1) \,|\, a, b \in \mathbb{R}\} \\
&= \{(a+b, a, b) \,|\, a, b \in \mathbb{R}\} \\
&= \{(x,y,z) \,|\, x - y - z = 0 \ , \ x, y, z \in \mathbb{R}\} \ .
\end{aligned}
$$

Für $S' = \{(1,1,0), (2,1,1)\}$ gilt $[S'] = [S]$.

4.6. Beispiel. Es sei $V = P_\infty(\mathbb{R})$, $S = \{1, x^2, x^4, \ldots, x^{2n}, \ldots\}$. Dann gilt $[S] = \{p(x) \in P_\infty(\mathbb{R}) \,|\, p(-x) = p(x)\}$.

4.7. **Definition.** Es sei V ein Vektorraum über F. Eine nicht leere Untermenge W von V heisst *Unterraum* von V, wenn für $\alpha, \beta \in W$ und $a, b \in F$ stets gilt $a\alpha + b\beta \in W$.

Ist W ein Unterraum des Vektorraumes V über F, so ist W zusammen mit den in V definierten Operationen der Addition und der skalaren Multiplikation selbst ein Vektorraum über F.

4.8. Beispiele. $\{0\}$ und V sind trivialerweise Unterräume von V. Der Vektorraum $P_m(\mathbb{R})$ ist für $m \leq n$ Unterraum von $P_n(\mathbb{R})$. Ist $c \in [0,1]$, so ist $\{f \in C[0,1] \,|\, f(c) = 0\}$ ein Unterraum von $C[0,1]$. Der Lösungsraum eines homogenen linearen Gleichungssystems über F mit n Unbekannten ist ein Unterraum von F^n.

4.9. **Satz.** *Es sei S eine Familie von Vektoren aus V. Dann ist $[S]$ der kleinste Unterraum W von V, der S umfasst.*

Beweis. Es ist klar, dass $[S]$ die Vektoren von S enthält. Mit α und β ist auch $a\alpha + b\beta$ Linearkombination von Vektoren aus S. Damit ist $[S]$ ein Unterraum, der S umfasst.

Umgekehrt liegen alle Linearkombinationen von Vektoren aus S im Unterraum W. Damit ist $[S]$ der *kleinste* Unterraum, der S umfasst.

4.10. **Satz.** *Ist β eine Linearkombination von Vektoren aus S, so gilt $[S] = [S \cup \beta]$.*

Beweis. Als Linearkombination von Vektoren aus S liegt β in $[S]$. Damit ist $[S]$ ein Unterraum, der sowohl S als auch β enthält. Nach Satz 4.9 folgt $[S \cup \beta] \subseteq [S]$. Umgekehrt gilt natürlich $[S] \subseteq [S \cup \beta]$. Damit ist der Satz bewiesen.

4.11. **Definition.** Man sagt, $[S]$ werde von S *aufgespannt* oder von S *erzeugt*. Gilt $[S] = V$, so heisst S ein *Erzeugendensystem* von V. Ein Vektorraum V, für den ein endliches Erzeugendensystem existiert, heisst *endlich erzeugbar*.

4.12. Beispiel. Es sei A eine $m \times n$-Matrix über dem Körper F. Man kann die Spalten von A als Vektoren von F^m auffassen. Der von diesen in F^m erzeugte Unterraum heisst *Spaltenraum* von A. Ebenso kann man die Zeilen von A als Vektoren in F^n auffassen. Der von ihnen in F^n erzeugte Unterraum heisst *Zeilenraum* von A.

4.13. Beispiel. Es sei $V = \mathbb{R}^n$, $S = \{\epsilon_1, \ldots, \epsilon_n\}$,

$$\begin{aligned}
\epsilon_1 &= (1, 0, 0, \ldots, 0) \\
\epsilon_2 &= (0, 1, 0, \ldots, 0) \\
\epsilon_3 &= (0, 0, 1, \ldots, 0) \\
&\vdots \\
\epsilon_n &= (0, 0, 0, \ldots, 1)\ .
\end{aligned}$$

Dann ist $[S] = V$, und S ist ein Erzeugendensystem von V. Für $\alpha = (a_1, \ldots, a_n)$ gilt

$$\alpha = \sum_{i=1}^{n} a_i \epsilon_i\ .$$

Insbesondere ist $\mathbb{R}^n$ endlich erzeugt.

4.14. Beispiel. Es sei $V = P_\infty(\mathbb{R})$, $S = \{1, x, x^2, \ldots, x^n, \ldots\}$. Dann ist S ein Erzeugendensystem, denn jedes Polynom ist Linearkombination der Standardpolynome $1, x, x^2, \ldots$. Wir überlassen es dem Leser zu zeigen, dass $P_\infty(\mathbb{R})$ nicht endlich erzeugbar ist.

4.15. **Satz.** *Der Durchschnitt einer nicht leeren Familie von Unterräumen von V ist wieder ein Unterraum von V.*

Beweis. Es sei W_i, $i \in I$ eine nicht leere Familie von Unterräumen von V. Ist $\alpha, \beta \in \bigcap W_i$, so gilt $\alpha, \beta \in W_i$ für alle $i \in I$. Da W_i ein Unterraum ist, folgt $a\alpha + b\beta \in W_i$ für alle $a, b \in F$. Damit gilt $a\alpha + b\beta \in \bigcap W_i$, und der Satz ist bewiesen.

Wir bemerken, dass die Vereinigung von Unterräumen im allgemeinen *kein* Unterraum ist. Hingegen gilt die entsprechende Aussage für die sogenannte *Summe* von Unterräumen.

4.16. **Definition.** Es seien $W_1, W_2, \ldots, W_p$ Unterräume des Vektorraumes V über F. Dann ist die *Summe* $W_1 + W_2 + \cdots + W_p$ definiert durch

$$W_1 + W_2 + \cdot + W_p = \{\alpha_1 + \alpha_2 + \cdots + \alpha_p \,|\, \alpha_i \in W_i \ , \quad i = 1, \ldots, p\} \ .$$

4.17. **Satz.** *Die Summe W, $W = W_1 + W_2 + \cdots + W_p$ der Unterräume $W_1, W_2, \ldots, W_p$ des Vektorraumes V über F ist der kleinste Unterraum von V, der jedes der W_i enthält.*

Beweis. Wir zeigen zuerst, dass W ein Unterraum ist. Es sei $\alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_p$, $\beta = \beta_1 + \beta_2 + \cdots + \beta_p$, $\alpha_i, \beta_i \in W_i$. Dann gilt für alle $a, b \in F$

$$a\alpha + b\beta = (a\alpha_1 + b\beta_1) + (a\alpha_2 + b\beta_2) + \cdots + (a\alpha_p + b\beta_p) \in W \ .$$

Damit ist W ein Unterraum. Es ist klar, dass W jedes W_i, $i = 1, \ldots, p$ enthält. Es bleibt zu zeigen, dass W der kleinste solche Unterraum ist. Es sei also W' ein Unterraum von V, der jedes der W_i umfasst. Es sei $\alpha_1 \in W_1, \ldots, \alpha_p \in W_p$. Dann ist $\alpha_i \in W'$, $i = 1, \ldots, p$, da W_i in W' enthalten ist. Da W' ein Unterraum ist, folgt $\alpha_1 + \alpha_2 + \cdots + \alpha_p \in W'$. Dies bedeutet $W \subseteq W'$. Damit ist der Satz bewiesen.

4.18. **Übungsaufgaben.**
1. Man beweise, dass $P_\infty(\mathbb{R})$ nicht endlich erzeugbar ist (siehe 4.14).
2. Die Teilmengen T_i, $i = 1, 2, \ldots, 5$ von $\mathbb{R}^4$ seien wie folgt definiert:

(a) $T_1 = \{(a_1, a_2, a_3, a_4) \,|\, a_1 \neq 0\}$,

(b) $T_2 = \{(a_1, a_2, a_3, a_4) \,|\, a_1 + a_3 = 0 \text{ und } a_2 + a_4 = 0\}$,

(c) $T_3 = \{(a_1, a_2, a_3, a_4) \,|\, a_1 - a_3 = 0 \text{ oder } a_2 - a_4 = 0\}$,

(d) $T_4 = \{(a_1, a_2, a_3, a_4) \,|\, a_1^2 - 2a_1a_3 + a_3^2 = a_4^2\}$,

(e) $T_5 = \{(a_1, a_2, a_3, a_4) \,|\, a_1 \in \mathbb{Q}\}$.

Welche dieser Teilmengen sind Unterräume von $\mathbb{R}^4$?
3. Es sei V der Vektorraum über $\mathbb{R}$ der reellwertigen Funktionen, die auf $[-1, 1]$ definiert sind. Welche der folgenden Teilmengen X_i sind Unterräume?

(a) $X_1 = \{f \in V \,|\, f(0) = f(1)\}$,

(b) $X_2 = \{f \in V \,|\, f(x) = -f(-x) \text{ für alle } x \in [-1, 1]\}$,

(c) $X_3 = \{f \in V \,|\, f(x^2) = (f(x))^2 \text{ für alle } x \in [-1, 1]\}$.

4. Es seien S und T zwei Familien von Vektoren des Vektorraumes V. Man beweise:

   (a) Es gilt $[S] = [T]$ genau dann, wenn jeder Vektor aus S eine Linearkombination von Vektoren aus T ist und jeder Vektor aus T eine Linearkombination von Vektoren aus S ist.

   (b) Es gilt $[S] + [T] = [S \cup T]$.

I.5. Vektorräume über beliebigen Körpern

Wir haben bis anhin viele Beispiele von Vektorräumen über den reellen, komplexen oder rationalen Zahlen kennengelernt. Wie weiter oben bereits kurz erwähnt, kann man allgemeiner Vektorräume über einem beliebigen sogenannten *Körper* F betrachten. Ein Körper ist dabei als ein algebraisches Objekt definiert, in dem eine Addition und eine Multiplikation gegeben ist, die gewissen Gesetzen genügen. Für $\mathbb{R}$, $\mathbb{C}$ und $\mathbb{Q}$ sind diese Gesetze alle wohlbekannt. – Wenn nicht ausdrücklich etwas anderes gesagt wird, so gelten die in den folgenden Kapitel bewiesenen Sätze der linearen Algebra für Vektorräume über einem beliebigen Körper.

5.1. **Definition.** Eine Menge F, zusammen mit einer Addition "+" und einer Multiplikation "$\cdot$" heisst *Körper*, falls die folgenden Axiome für alle $a, b, c \in F$ erfüllt sind:

(F1) $a + b = b + a$;

(F2) $a + (b + c) = (a + b) + c$;

(F3) es existiert ein eindeutig bestimmtes Element $0 \in F$ mit $a + 0 = a$ für alle a ;

(F4) zu $a \in F$ existiert ein eindeutig bestimmtes Element $-a \in F$ derart, dass gilt $a + (-a) = 0$;

(F5) $a \cdot b = b \cdot a$;

(F6) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

(F7) es existiert ein eindeutig bestimmtes Element $1 \in F$ mit $1 \neq 0$ und $a \cdot 1 = a$ für alle $a \in F$;

(F8) zu $a \in F$, $a \neq 0$ existiert ein eindeutig bestimmtes Element $a^{-1} \in F$ mit $a \cdot a^{-1} = 1$;

(F9) $a \cdot (b + c) = a \cdot b + a \cdot c$.

Die Axiome F1, F2,…, F4 betreffen die Addition, F5, F6,…, F8 die Multiplikation, und F9 betrifft die Verknüpfung der beiden Operationen (*Distributivität*). F1 und F5 besagen, dass die Addition bzw. Multiplikation *kommutativ* ist. F2 und F6 besagen, dass die Addition bzw. Multiplikation *assoziativ* ist.

5.2. Beispiele. $\mathbb{R}$, $\mathbb{C}$ und $\mathbb{Q}$ zusammen mit der üblichen Addition und Multiplikation sind Körper. Die ganzen Zahlen $\mathbb{Z}$ bilden keinen Körper, denn das Axiom F8 ist nicht erfüllt: zum Beispiel existiert zu 2 kein multiplikatives Inverses! Die Menge F, definiert durch $F = \{a + b\sqrt{3} \,|\, a, b \in \mathbb{Q}\} \subset \mathbb{R}$ mit der üblichen Addition und Multiplikation von reellen Zahlen ist ein Körper.

5.3. Beispiel. Es sei p eine Primahl. Der Primkörper $\mathbb{F}_p$ ist wie folgt definiert:

$$\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\} \ .$$

Für Zahlen a, b mit $0 \le a, b \le p-1$ gibt es eindeutig bestimmte Zahlen m, n und k, l mit $a + b = mp + k$, $a \cdot b = np + l$ und $0 \le k, l \le p-1$. (Division von $a + b$ bzw. $a \cdot b$ durch p mit Rest.)

Wir definieren die Addition und die Multiplikation in $\mathbb{F}_p$ durch

$$a +_p b = k \ , \quad a \cdot_p b = l \ .$$

Wir überlassen es dem Leser zu zeigen, dass $\mathbb{F}_p$ damit zu einem Körper wird.

5.4. **Satz.** *Es sei F ein Körper. Dann gilt für $a, b \in F$:*

(i) $0 \cdot a = a \cdot 0 = 0$ *;*

(ii) $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$ *;*

(iii) $-(-a) = a$ *;*

(iv) $(a^{-1})^{-1} = a$ *;*

(v) $(-1) \cdot a = -a$ *;*

(vi) $(-a) \cdot (-b) = a \cdot b$ *.*

Beweis. (i): Es gilt $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$. Daraus folgt $0 = 0 \cdot a$ nach Addition von $-(0 \cdot a)$ auf beiden Seiten. Ebenso beweist man $a \cdot 0 = 0$.
(v): Es gilt $a + (-1) \cdot a = 1 \cdot a + (-1) \cdot a = (1 + (-1)) \cdot a = 0 \cdot a = 0$ nach (i). Daraus folgt

mit F4 sofort $(-1) \cdot a = -a$.
(vi): Einerseits folgt aus $a + (-a) = 0$ durch Multiplikation mit $(-b)$

$$a \cdot (-b) + (-a)(-b) = 0 \cdot (-b) = 0 \ ;$$

andererseits folgt aus $(-b) + b = 0$ durch Multiplikation mit a

$$a \cdot (-b) + a \cdot b = a \cdot 0 = 0 \ .$$

Daraus ergibt sich unter Anwendung von F4 sofort

$$(-a) \cdot (-b) = a \cdot b \ .$$

Die Aussagen (ii), (iii), (iv) zu beweisen überlassen wir dem Leser.

5.5. **Übungsaufgaben.**

1. Man verifiziere die in Beispiel 5.3 gemachten Aussagen. Für $p = 2$ und $p = 3$ beschreibe man die Operationen in $\mathbb{F}_p$ explizit.
2. Man vervollständige den Beweis von Satz 5.4.
3. Man bestimme alle Teilmengen von $\mathbb{Q}$, welche bezüglich $+$ und $\cdot$ die Körperaxiome erfüllen.
4. Man überzeuge sich, dass die in Abschnitt I.1 gemachten Aussagen über lineare Gleichungssysteme und Matrizen sinngemäss für einen beliebigen Körper an Stelle von $\mathbb{R}$ gelten. (Vorsicht mit Satz 1.7.ii.)