REPETITORIUM LINEARE ALGEBRA 1

gehalten von

Lars Lauer und Jonas Metzinger

vom 25.03.24 bis 28.03.24

Skript wurde verfasst von

Maximilian Leist und Jonas Metzinger

Mathematik Fachschaft

Website: `https://mathwp.fsr.saarland/`

Instagram: `https://instagram.com/fsmatheuds/`

E-Mail: fsmathe@math.fs.uni-saarland.de

Hinweise

Dieses Skript hat keinen Anspruch auf Vollständigkeit und Fehlerfreiheit, da es von studentischer Seite zum Zwecke des Repetitorums erstellt wurde.

In diesem Skript sei die naive Logik und Mengenlehre vorausgesetzt. Auf Beweise wird aus Zeitgründen in diesem Skript und dem Repetitorium bewusst größtenteils verzichtet. Dennoch sei ausdrücklich erwähnt, dass Beweise klar zum Verständnis beitragen, daher empfehlen wir beim Lernen sich dennoch auch Beweise anzuschauen und diese auch nach zu vollziehen, um das mathematische Verständnis zu festigen.

Hinweise auf Fehler sind erwünscht:

s8jometz@stud.uni-saarland.de

Fehler können auch via Microsoft Teams per private Nachricht an Jonas Metzinger gemeldet werden.

Inhaltsverzeichnis

Kapitel I.

Relationen, Gruppen und Körper

1. Relationen

Definition I.1.1 (Relation): Sei M eine Menge. Eine Teilmenge $\mathfrak{R} \subseteq M \times M$ heißt zweistellige (binäre) Relation auf M. Man schreibt statt $(x, y) \in \mathfrak{R}$ auch $x\mathfrak{R}y$.[1]

Beispiel I.1.2:

(i) Sei M eine Menge. Definiere $\mathfrak{R}_1 := \{(x, y) \in M^2 \mid x = y\}$. Diese Relation nennen wir die Gleichheitsrelation.

(ii) Sei M die Menge der Teilnehmer an diesem Repetitorium, dann definiert $\mathfrak{R}_2 := \{(s_1, s_2) \in M^2 \mid s_1 \text{ und } s_2 \text{ haben im selben Monat Geburtstag}\}$ eine Relation auf M.

Von Bedeutung sind insbesondere Relationen, die folgende Eigenschaften erfüllen.

Definition I.1.3 (Eigenschaften von Relationen): Sei M eine Menge und $\mathfrak{R}$ eine Relation auf M.

(i) Gilt für alle $x \in M$, dass $x\mathfrak{R}x$, dann heißt $\mathfrak{R}$ reflexiv.

(ii) Gilt für alle $x, y \in M$ mit $x\mathfrak{R}y$, dass $y\mathfrak{R}x$, dann heißt $\mathfrak{R}$ symmetrisch.

(iii) Gilt für alle $x, y \in M$ mit $x\mathfrak{R}y$ und $y\mathfrak{R}x$, dass $x = y$, dann heißt $\mathfrak{R}$ antisymmetrisch.

(iv) Gilt für alle $x, y, z \in M$ mit $x\mathfrak{R}y$ und $y\mathfrak{R}z$, dass $x\mathfrak{R}z$, dann heißt $\mathfrak{R}$ transitiv.

[1] Häufig sieht man auch $\sim$ oder $\leq$ als Symbol für die Relation. Dies sieht dann nicht mehr so ungewohnt aus.

Mit diesen Begriffen lassen sich jetzt vertraute Relationen besser klassifizieren.

Definition I.1.4 (Äquivalenz- und partielle Ordnungsrelation): Sei M eine Menge und $\mathfrak{R}$ eine Relation auf M.

(i) Ist $\mathfrak{R}$ reflexiv, symmetrisch und transitiv, dann nennen wir $\mathfrak{R}$ eine Äquivalenzrelation. Häufig sieht man hierfür das Symbol „$\sim$“.

(ii) Ist $\mathfrak{R}$ reflexiv, antisymmetrisch und reflexiv, dann nennen wir $\mathfrak{R}$ eine (partielle) Ordnungsrelation. Häufig sieht man hierfür „$\leq$“ als Symbol.

Wir betrachten nun zwei „berühmte“ Beispiele von solchen besonderen Relationen.

Beispiel I.1.5 (Kongruenzrelation und Teilbarkeitsrelation):

(i) Sei $M = \mathbb{N}$, definiere

$$\mathfrak{R}_t := \{(x, y) \in \mathbb{N}^2 \mid x \text{ teilt } y, \text{ bzw. es existiert ein } k \in \mathbb{N} \text{ mit } y = kx\}$$

Diese Relation nennen wir auch Teilbarkeitsrelation und notieren für $x\mathfrak{R}_t y$ auch $x \mid y$. Seien z. B. $a = 3$, $b = 5$ und $c = 15$, dann $a \mid c$, $b \mid c$ aber $a \nmid b$

(ii) Sei n eine natürliche Zahl. Wir definieren

$$\mathfrak{R}_s := \{(x, y) \in \mathbb{Z}^2 \mid x - y \text{ ist durch } n \text{ teilbar}\}$$

Diese Relation heißt auch *Kongruenz modulo n*. Notiere für $(x, y) \in \mathfrak{R}_s$ auch $x \equiv y \pmod{n}$. Seien so z. B. $n = 6$, $y = 10$. Durch Division von y durch n bekommen wir als Rest 4 raus, d. h. $4 \equiv 10 \pmod 6$, bzw. $4\mathfrak{R}_s 10$ (da $4 - 10 = -6$ und 6 teilt -6).

Bemerkung I.1.6:

(i) Die Kongruenzrelation ist eine Äquivalenzrelation, während es sich bei der Teilbarkeitsrelation um eine partielle Ordnungsrelation handelt.

(ii) Weitere offensichtliche Ordnungsrelationen sind beispielsweise auf $\mathbb{Z}$ gegeben durch $\leq$ und $\geq$.

(iii) Gemäß Beispiel gilt $4\mathfrak{R}_s 10$ für $n = 6$. Es gilt aber ebenso $10\mathfrak{R}_s 10$, allgemeiner gilt $(4 + 6k)\mathfrak{R}_s 10$ mit $k \in \mathbb{Z}$.

Schreibe folglich allgemein für $0 \leq i \leq n - 1$

$$M_i := \{x \in \mathbb{Z} \mid x \equiv i \pmod{n}\} = \{i + kn \mid k \in \mathbb{Z}\} = [i]_n$$

Wir nennen diese M_i Restklassen bezüglich dem „Teilen mit Rest durch n “.

Im Fall von beliebigen Äquivalenzrelationen definieren wir *Äquivalenzklassen* wie folgt

Definition I.1.7 (Äquivalenzklasse, Menge der Äquivalenzklassen): Sei M eine Menge und $\sim$ eine Äquivalenzrelation. Für $x \in M$ heißt

$$[x]_\sim := \{y \in M \mid x \sim y\} \subseteq M$$

Äquivalenzklasse von x bzgl. $\sim$.

Die Menge

$$M/\sim := \{[x]_\sim \mid x \in M\}$$

nennen wir die *Menge aller der Äquivalenzklassen* von M bzgl. $\sim$.

Die Abbildung $\pi\colon M \to M/\sim$, $x \mapsto [x]_\sim$ nennen wir kanonische Projektion.

Nun wollen wir ein paar Eigenschaften in aller Kürze sammeln um eine weitere Möglichkeit der Beschreibung einer Äquivalenzrelation zu bekommen.

Proposition I.1.8: *Sei M eine Menge und $\sim$ eine Äquivalenzrelation auf M. Seien weiterhin $x, y \in M$*

(i) *Es gilt $x \in [x]$, insbesondere $[x] \neq \emptyset$*

(ii) *Es gilt $x \sim y$ genau dann, wenn $[x] = [y]$. Insbesondere sind Äquivalenzklassen disjunkt, d. h. für $x, y \in M$ gilt entweder $[x] = [y]$ oder $[x] \cap [y] = \emptyset$.*

(iii) *M ist die Vereinigung seiner Äquivalenzklassen, d. h. $M = \bigcup_{x \in M} [x]$.*

Aus ii) und iii) bekommen wir den Begriff der Partition.

Definition I.1.9 (Partition): Sei M eine Menge und $P \subseteq \mathfrak{P}(M)$. Gilt

(i) Die leere Menge ist kein Element in P,

(ii) Es gilt $\bigcup_{A \in P} A = M$,

(iii) Für $A, B \in P$ gilt $A = B$ oder $A \cap B = \emptyset$,

so heißt P eine Partition von M.

Bemerkung I.1.10:

(i) Offensichtlich bilden die Äquivalenzklassen eine Partition.

(ii) Man kann als Aussage ebenso zeigen, dass wir mit einer gegebenen Partition P uns dadurch eine Äquivalenzrelation $\sim_P$ definieren können.

Exkurs: Wohldefiniertheit

Seien M, N Mengen und $f\colon M \to N$ eine Abbildung. Weiterhin sei $\sim$ eine Äquivalenzrelation und es bezeichne $M/{\sim}$ die Menge aller Äquivalenzklassen. Dann heißt eine Abbildung $\tilde{f}\colon M/{\sim} \to N, [x]_\sim \to f(x)$ genau dann *wohldefiniert*, wenn für alle $x \sim y$ gilt $\tilde{f}([x]_\sim) = f(x) = \tilde{f}([y]_\sim) = f(y)$.

Intuitiv heißt es, dass unabhängig davon welchen *Repräsentanten* wir wählen, das selbe Bild rauskommen soll. Wir wollen dies an Beispielen aus der Gruppentheorie (folgender Abschnitt) illustrieren:

Beispiel I.1.1: (i) Sei $\phi\colon \mathbb{Z}/15\mathbb{Z} \to S_4, [n]_{15} \mapsto (1,2,3)^n$. Beachte, dass die Ordnung der Permutation $(1,2,3)$ gegeben ist durch 3, d. h. $(1,2,3)^3 = \mathrm{id}$. Zeige, dass die Abbildung ϕ wohldefiniert ist.

Beweis: Seien $n, m \in \mathbb{Z}$ mit $[n] = [m]$ (z. B. $[16] = [1] = [-14]$). Nach Definition existiert $k \in \mathbb{Z}$, sodass $m = n + 15k$. Es gilt

$$\begin{aligned}\phi([m]) &= (1,2,3)^m = (1,2,3)^{n+15k} = (1,2,3)^n(1,2,3)^{15k}\\ &= (1,2,3)^n\left((1,2,3)^3\right)^{5k} = (1,2,3)^n\,\mathrm{id}^{5k}\\ &= (1,2,3)^n = \phi([n]).\end{aligned}$$

□

(ii) Sei $\phi\colon \mathbb{Z}/15\mathbb{Z} \to S_4, [n]_{15} \mapsto (1,2)^n$. Diese Abbildung ist nicht wohldefiniert, da $[1] = [16]$ aber $\phi([1]) = (1,2)$ und $\phi([16]) = (1,2)^{16} = \left((1,2)^2\right)^8 = \mathrm{id}^8 = \mathrm{id}$.

2. Gruppen

In der Linearen Algebra und insbesondere der Algebra interessieren wir uns für bestimmte algebraische Strukturen, die wir teilweise auch bereits kennen. Um deren Eigenschaften noch besser zu begreifen, müssen wir hierbei deutlich abstrakter vorgehen und wichtige strukturelle Eigenschaften herausstellen.

Definition I.2.1 (Verknüpfungen): Sei M eine Menge.

(i) Eine Abbildung $\star\colon M \times M \to M$ heißt (binäre) Verknüpfung auf M. Schreibe üblicherweise $m_1 \star m_2 := \star(m_1, m_2)$.

(ii) Gilt für alle $a, b, c \in M$, dass $a \star (b \star c) = (a \star b) \star c$, dann nennen wir $\star$ assoziativ.

(iii) Gilt für $a, b \in M$, dass $a \star b = b \star a$, dann nennen wir $\star$ kommutativ.

(iv) Existiert ein Element $e \in M$, sodass $a \star e = e \star a$ für alle $a \in M$ gilt, dann heißt e *neutrales Element*. Dieses ist eindeutig, denn $e' = e' \star e = e$.

(v) Sei $\star$ assozativ mit neutralem Element und sei $g \in M$. Existiert ein $h \in M$ mit $h \star g = g \star h = e$, dann heißt h inverses Element von g. Man kann ebenso deren Eindeutigkeit zeigen. Notiere $g^{-1} := h$.

Definition I.2.2 (Gruppen): Sei G eine Menge und $\star$ eine Verknüpfung auf G. Gilt

(i) Die Verknüpfung $\star$ ist assozativ,

(ii) Es existiert ein neutrales Element e bzgl. der Verknüpfung,

(iii) Für jedes $g \in G$ existiert ein inverses Element,

dann heißt $(G, \star)$ eine Gruppe.[2]
Ist $\star$ zusätzlich kommutativ, so nennen wir $(G, \star)$ eine abelsche Gruppe.

Beispiel I.2.3:

(i) $(\mathbb{Z}, +)$ mit der üblichen Addition ist eine abelsche Gruppe, mit neutralem Element „0“.

(ii) $(\mathbb{R}\backslash\{0\}, \cdot)$ mit der üblichen Multiplikation ist eine abelsche Gruppe, siehe auch den Abschnitt mit Körpern.

(iii) $(\mathbb{N}, +)$ ist keine Gruppe, da z. B. die 2 kein additives Inverses in $\mathbb{N}$ besitzt.

(iv) Sei $n \in \mathbb{N}$. Die Menge $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], [2], \ldots, [n-1]\}$ versehen mit der Addition $[a] + [b] = [a + b]$ bildet eine Gruppe, wobei $[i]$ die Äquivalenzklasse von i bzgl. Kongruenz $\pmod{n}$ bezeichnet. Die sogenannte *Gruppe der Kongruenzklassen.*

Definition I.2.4 (Untergruppe): Sei $(G, \star)$ eine Gruppe und H eine Teilmenge von G. Falls gilt

(i) Das neutrale Element e von G ist in H,

(ii) Für $g, h \in H$ gilt auch $g \star h \in H$,

(iii) Für $h \in H$ ist auch $h^{-1} \in H$,

[2] Ist klar welche Verknüpfung gemeint ist, so schreibt man häufig nur „G ist eine Gruppe“. Bei multiplikativen Verknüpfungen spart man sich generell gerne die Verknüpfungszeichen

dann nennen wir H Untergruppe von G. Eine Untergruppe H ist ebenso eine Gruppe mit der auf H eingeschränkten Verknüpfung der ursprünglichen Gruppe G.

Etwas handlicher erscheint dieses Kriterium.

Proposition I.2.5 (Untergruppenkriterium): *Sei $(G, \star)$ eine Gruppe und H eine Teilmenge von G. H ist eine Untergruppe genau dann, wenn*

(i) *H ist nicht leer und*

(ii) *Für $g, h \in H$ ist $g \star h^{-1} \in H$.*

Definition I.2.6 (Ordnung): Sei G eine Gruppe und $g \in G$. Wir bezeichen $\operatorname{ord}(G) = \#G$ als die Ordnung von G. Weiterhin bezeichnen wir $\operatorname{ord}(g) = \#\langle g \rangle$ als Ordnung des Elements g.

Beispiel I.2.7: Sei $(\mathbb{Z}/5\mathbb{Z}, +)$ und sei $[2] \in \mathbb{Z}/5\mathbb{Z}$, dann $\langle [2] \rangle = \{[2], [4], [1], [3], [0]\}$, d. h. $\langle [2] \rangle = \mathbb{Z}/5\mathbb{Z}$ und $[2]$ hat Ordnung 5.

Definition I.2.8 (Nebenklassen): Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Definiere folgende Äquivalenzrelation

$$x \sim y \Leftrightarrow \exists\, h \in H \text{ mit } x = yh.$$

Für die Äquivalenzklasse von $x \in G$ schreibt man xH und nennt dies die Linksnebenklasse von $x \in G$.

Analog bekommen wir die Rechtsnebenklasse von $x \in G$. Hierbei schreiben wir Hx für die Äquivalenzklasse.

Satz 1 (Satz von Lagrange): *Sei $(G, \star)$ eine endliche Gruppe, und $U \leq G$ eine Untergruppe, dann teilt die Ordnung von U die Ordnung von G.*[3]

Korollar I.2.9 (Zyklische Gruppe mit prim Ordnung): *Sei p eine Primzahl und G eine endliche Gruppe mit Primzahlordnung. Dann ist G zyklisch.*

In der Strukturmathematik interessieren wir uns v. a. für strukturerhaltende Abbildungen mit denen wir beispielweise unterschiedliche Gruppen in Beziehung setzen können. In der Kategorie der Gruppen sind dies die Gruppenhomomorphismen, die wir wie folgt definieren.

[3] In der Literatur findet man häufig eine andere Formulierung mit Hilfe des Begriffes des Index. Hiermit wird die Mächtigkeit der Links- bzw. Rechtsnebenklasse von G/U respektive $U \backslash G$ bezeichnet.

Definition I.2.10 (Gruppenhomomorpismus): Seien $(G, *)$ und $(H, \star)$ zwei Gruppen. Eine Abbildung $f\colon (G, *) \to (H, \star)$ mit $f(g * h) = f(g) \star f(h)$ für alle $g, h \in G$ heißt Gruppehomomorphismus. Man sagt f ist verträglich bzgl. der Strukturen von G und H.

Ist f bijektiv[4], so sprechen wir von einem *Isomorphismus*.

Sind beide Gruppen gleich, reden wir von einem *Endomorphismus* und sollte f sogar bijektiv sein, so reden wir von einem *Automorphismus*.

3. Die Symmetrische Gruppe

Definition I.3.1 (Symmetrische Gruppe): Sei M eine Menge. Wir definieren $\mathrm{Sym}(M) := \{f\colon M \to M \mid f \text{ ist bijektiv}\}$.

Insbesondere wollen wir den Spezialfall, in dem M endlich ist. In diesem können wir die Elemente durchnummerieren, sagen wir beispielsweise $M = \{m_1, \ldots, m_n\}$.

$$S_n := \mathrm{Sym}(\{1, 2, \ldots, n\}) = \{\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} \mid \sigma \text{ ist bijektiv}\}$$

Mit der Komposition/Verkettung $\circ$ als Verknüpfung bekommen wir eine Gruppe.

Die Symmetrischen Gruppe ist v. a. in der Algebra von besonderer Bedeutung bei der Untersuchung von Nullstellen bei Polynomen innerhalb der Galoistheorie, aber auch bei anderen Problemen wie der Konstruierbarkeit mit Lineal und Zirkel.

Sie sind zusätzlich auch geometrisch gut zu verstehen als Drehungen von Figuren wie n-Ecken, daher kommt ihnen auch in der modernen Algebra immer noch eine hohe Bedeutung zu Gute.

Bemerkung I.3.2 (Zykelschreibweise von Permutationen): Wir notieren eine Permutation $\sigma \in S_n$ mit

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

Diese Schreibweise hat Vorteile ist aber umständlich, wir wollen daher eine bessere Möglichkeit haben Permutation zu notieren. Hierzu nehme man ein $a \leq n$ und bilde

$$(a\, \sigma(a)\, \sigma^2(a)\, \ldots \sigma^{k-1}(a))$$

[4]Dies gilt „zufällig“ bei Gruppen. Je nach Kategorie muss dies aber nicht gelten. Allgemeiner verlangt man die Existenz eines Inversen.

wobei k so gewählt ist, dass $\sigma^k(a) = a$. Wir nennen diese „Klammer" *k-Zyklus* So können wir jede Permutation als Verknüpfung von diesen Zyklen schreiben, indem wir systematisch die $a \leq n$ durchgehen, wobei (a) bedeutet, dass es fixiert ist unter dieser Permutation.

Beispiel I.3.3: Sei

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 2 & 3 \end{pmatrix}$$

Wir starten mit der 1. Diese wird auf die 1 geschickt.

Jetzt betrachten wir die 2, diese wird geschickt auf 4, d. h. $\sigma(2) = 4$. Die 4 wird geschickt auf die 2, d. h. $\sigma(4) = 2 = \sigma^2(2)$. Also bekommen wir den Zyklus $(2\,4)$. Analog bekommen wir $(3\,5)$.

Ingesamt bekommen wir $\sigma = (1)(2\,4)(3\,5) = (2\,4)(3\,5)$.

Definition I.3.4 (Signums-Funktion): Sei $n \in \mathbb{N}$ und $\sigma \in S_n$. Wir bezeichnen

$$\operatorname{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

als Signum von σ. Wir bekommen eine Abbildung $\operatorname{sgn}\colon S_n \to \{\pm 1\}$.

Diese Abbildung ist ein Gruppenhomomorphismus (nachrechnen!).

Beispiel I.3.5: (i) Sei $\pi \in S_n$, dann

$$\operatorname{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(\pi(j)) - \sigma(\pi(i))}{\pi(j) - \pi(i)}$$

(ii) Sei $\sigma = (1\;2\;3) \in S_3$. Wir bestimmen $\operatorname{sgn}(\sigma)$.

$$\operatorname{sgn}(\sigma) = \prod_{1 \leq i < j \leq 3} \frac{\sigma(j) - \sigma(i)}{j - i} = \frac{\sigma(2) - \sigma(1)}{2 - 1} \cdot \frac{\sigma(3) - \sigma(1)}{3 - 1} \cdot \frac{\sigma(3) - \sigma(2)}{3 - 2} = 1$$

(iii) Man möchte natürlich nicht immer so aufwendig rumrechnen müssen. Es lässt sich zeigen, dass wir für einen Zyklus σ der Länge k folgende Beziehung bekommen

$$\operatorname{sgn}(\sigma) = \begin{cases} -1, & \text{falls } k \text{ gerade} \\ 1, & \text{sonst.} \end{cases}$$

4. Ringe und Körper

In diesem Abschnitt wollen wir kurz den Begriff des Ringes einführen. Ringe finden innerhalb der Algebra, beispielsweise der algebraischen Zahlentheorie, eine große Bedeutung.

Definition I.4.1 (Ringe): Sei R eine Menge mit zwei Verknüpfungen „+“ und „$\cdot$“. Falls gilt

(i) $(R, +)$ ist eine abelsche Gruppe,

(ii) „$\cdot$“ ist assoziativ,

(iii) die Distributivgesetze gelten, d. h. für alle $x, y, z \in R$ gilt

$$x \cdot (y + z) = x \cdot y + x \cdot z \text{ und } (y + z) \cdot x = y \cdot x + z \cdot x,$$

dann heißt $(R, +\cdot)$ *Ring*.

Ist „$\cdot$“ kommutativ, so heißt der Ring kommutativ.

Existiert weiterhin ein Element $1_R \in R$, sodass für alle $x \in R$ die Gleichheit $1_R \cdot x = x \cdot 1_R = x$ gilt, dann heißt $(R, +, \cdot)$ *Ring mit Eins*.

Bemerkung I.4.2: Wir bezeichnen „+“ als Addition des Ringes und „$\cdot$“ als Multiplikation des Ringes. Das neutrale Element der Addition bezeichnen wir mit 0_R und nennen es *Nullelement*.

Ist unser Ring mit Eins, dann heißt 1_R auch *Einselement*. Ist weiterhin ein Element $y \in R$ invertierbar bzgl. der Multiplikation, so schreiben wir auch $1/y := y^{-1}$.

Beispiel I.4.3: (i) Die ganzen Zahlen $\mathbb{Z}$ mit der gewöhnlichen Multiplikation und Addition bilden einen kommutativen Ring mit Eins.

(ii) Die Menge $\mathbb{Z}/n\mathbb{Z}$ mit der Addition $[a]+[b] = [a+b]$ und der Multiplikation $[a] \cdot [b] = [a \cdot b]$ bilden einen kommutativen Ring mit Eins.

(iii) Sei X eine beliebige Menge. Dann ist $(\mathfrak{P}(X), \Delta, \cap)$ ein kommutativer Ring mit Eins. Hierbei bezeichne $\mathfrak{P}(X)$ die Potenzmenge von X und Δ die symmetrische Differenz definiert durch $A\Delta B := (A\backslash B) \cup (B\backslash A)$. Hierbei ist Δ die Addition und $\cap$ die Multiplikation. Die leere Menge ist das Nullelement und X das Einselement.

Genau wie bei Gruppen interessieren wir uns für *strukturerhaltende Abbildungen*, d. h. Abbildungen, die verträglich mit den Additionen und der Multiplikationen der Ringe sind.

Definition I.4.4 (Ringhomomorphismus): Seien $(R, +_R, \cdot_R)$ und $(S, +_S, \cdot_S)$ zwei Ringe. Eine Abbildung $\varphi\colon (R, +_R, \cdot_R) \to (S, +_S, \cdot_S)$ heißt *Ringhomomorphismus*, wenn für alle $x, y \in R$

$$\varphi(x +_R y) = \varphi(x) +_S \varphi(y) \text{ und } \varphi(x \cdot_R y) = \varphi(x) \cdot_S \varphi(y)$$

gilt. Sind beide Ringe zusätzlich mit Eins und es gilt $\varphi(1_R) = 1_S$, dann heißt φ *Ringhomomorphismus mit Eins.*

Bemerkung I.4.5 (Analogie der Bezeichnungen): Genauso wie bei Gruppen sprechen wir, wenn wir eine Inverse finden, oder äquivalent der Ringhomomorphismus bijektiv ist, von einem *Ringisomorphismus.*

Sind beide Ringe gleich so heißt der Ringhomomorphismus auch *Ringendomorphismus.* Ist dieser bijektiv, dann sprechen wir von einem *Ringautomorphismus.*

Weiterhin bezeichne

$$\mathrm{Kern}(\varphi) := \{r \in R \mid \varphi(r) = 0_S\}$$

den *Kern des Ringhomomorphismus.*

Definition I.4.6 (Charakteristik): Sei $(R, +, \cdot)$ ein Ring. Definiere

$$\mathrm{char}(R) = \begin{cases} \min\{k \in \mathbb{N} \mid \underbrace{1_R + 1_R + \ldots + 1_R}_{\text{k-mal}} = 0_R\}, & \text{falls existent} \\ 0, & \text{sonst.} \end{cases}$$

Wir nennen diese Zahl die Charakteristik von K.

Beispiel I.4.7: Die reellen Zahlen, rationalen Zahlen und auch die komplexen Zahlen, versehen mit den gewöhnlichen Verknüpfungen, haben Charakteristik 0.

Beachte, dass es auch Ringe gibt, welche zwar eine Charakteristik ungleich 0 haben, aber dennoch unendlich viele Elemente besitzen.

Man sollte daher die Begriffe der Ordnung einer Gruppe und der Charakteristik nicht durcheinander bringen.

Bemerkung I.4.8: Als Intuition kann man sich folgendes merken, bzgl. der Charakteristik:

„Ist die Charakteristik eines Ringes Null, dann findet sich eine Kopie der ganzen Zahlen in diesem Ring. In Ringen mit endlicher Charakteristik findet sich keine Kopie der ganzen Zahlen, sondern eine Kopie von $\mathbb{Z}/p\mathbb{Z}$, wobei p prim ist.“

Definition I.4.9 (Einheitengruppe): Sei $(R, +, \cdot)$ ein Ring. Die Menge

$$R^\times := \{x \in R \mid X \text{ ist invertierbar}\}$$

ist eine Gruppe mit der Ringmultiplikation und der 1_R als neutralem Element. Wir sagen auch *Einheitengruppe* zu $R^\times$.

Nun wollen wir den für die Algebra wichtigen Begriff des Körpers (Englisch: *field*) einführen.

Definition I.4.10 (Körper): Sei $(K, +, \cdot)$ ein Ring. Gilt

(i) K ist kommutativ,

(ii) $1_K \neq 0_K$ und

(iii) $K^\times = K\backslash\{0_K\}$ (d. h. jedes Element ungleich 0_K ist invertierbar),

dann heißt $(K, +, \cdot)$ *Körper*.

Beispiel I.4.11:

(i) Die rationalen und reellen Zahlen versehen mit der gewohnten Addition und Multiplikation sind Körper.

(ii) $\mathbb{Q}^2$ versehen mit folgender Addition $+_{\mathbb{Q}^2}$ und Multiplikation $\cdot_{\mathbb{Q}^2}$

$$(a, b) +_{\mathbb{Q}^2} (c, d) = (a + c, b + d) \text{ und } (a, b) \cdot_{\mathbb{Q}^2} (c, d) = (ac + 2bd, ad + bc)$$

ist ein Körper. (Nachrechnen als freiwillige Aufgabe.)

Definition I.4.12 (Primkörper): Sei p eine Primzahl, so ist $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ ein Körper. Schreibe auch $\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$, wobei $\operatorname{char}(\mathbb{F}_p) = p$.

Man kann folgende Proposition zeigen.

Proposition I.4.13: *Sei K ein Körper. Dann hat K entweder prime Charakteristik oder sie ist gleich 0.*

In vielen Gebieten der Mathematik (wie z. B. in der Algebra, der Funktionentheorie, der Funktionalanalysis etc.) interessiert man sich für komplexe Zahlen, weshalb wir sie kurz einmal als Körper vorstellen wollen.

Definition I.4.14 (Körper der komplexen Zahlen): Betrachte $\mathbb{R}^2$ versehen mit der folgenden Addition und Multiplikation

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

Wir definieren nun $\mathbb{C} := (\mathbb{R}^2, +, \cdot)$ und nennen diesen Körper den Körper der komplexen Zahlen. Statt (a, b) schreiben wir auch $a + bi$ und nennen i die imaginäre Einheit.

Man kann sich die Frage stellen, warum es überhaupt sinnvoll ist die komplexen Zahlen zu betrachten, dies liegt mitunter im folgenden Ergebnis aus der Algebra, die auf Gauß zurückgeht.

Satz 2 (Fundamentalsatz der Algebra): *Jedes nicht-konstante Polynom $P \in \mathbb{C}[X]$ mit komplexen Vorfaktoren hat eine Nullstelle über den komplexen Zahlen. Insbesondere ist der Grad des Polynoms gleich der Anzahl der Nullstellen mit Vielfachheit.*

Anders formuliert: Die komplexen Zahlen sind algebraisch abgeschlossen.

Kapitel II.

Lineare Gleichungssysteme und Vektorräume

Sei in diesem Kapitel K stets ein Körper.

1. Matrizen

Definition II.1.1 (Matrizen): Seien $n, m \in \mathbb{N}$. Eine Abbildung

$$A : \{1, ..., n\} \times \{1, ..., m\} \to K$$

heißt $n \times m$-Matrix über K. Notiere A mit $A = (A(i,j))_{1 \leq i \leq n, 1 \leq j \leq m}$ und schreibe $a_{i,j} := A(i,j$

$$A = (a_{i,j}) = \begin{pmatrix} a_{1,1} & \dots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \dots & a_{n,m} \end{pmatrix} \tag{II.1}$$

Ist $n = m$, heißt A quadratisch, bezeichne weiterhin

$$K^{n \times m} := \{A \ : \ A \text{ ist } n \times m \,\text{Matrix über } K\}$$

Beispiel II.1.2: Beispiele für Matrizen sind

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & -1 \end{pmatrix} \in \mathbb{R}^{2\times 3}\,, \ B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \\ 3 & -2 \end{pmatrix} \in \mathbb{R}^{3\times 2}$$

für $n \in \mathbb{N}$ heißt

$$I_n = (\delta_{i,j}) = \begin{pmatrix} 1 & 0 & \dots & \dots & 0 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix} \in K^{n \times n}$$

Einheitsmatrix, weitere Notationen für I_n sind beispielsweise I, E, E_n.

Für $n, m \in \mathbb{N}$ heißt

$$0 = \begin{pmatrix} 0 & \dots & \dots & 0 \\ \vdots & & & \vdots \\ 0 & \dots & \dots & 0 \end{pmatrix} \in K^{n \times m}$$

Nullmatrix.

Definition II.1.3: Seien $n, m, k \in \mathbb{N}$ definiere für $A, B \in K^{n \times k}, C \in K^{k \times m}, \lambda \in K$ folgendes

(i) $A + B \in K^{n \times k}$ durch $(A + B)(i, j) = A(i, j) + B(i, j)$

(ii) $\lambda A \in K^{n \times k}$ durch $(\lambda A)(i, j) = \lambda A(i, j)$

(iii) $A \cdot C \in K^{n \times m}$ durch $(A \cdot C)(i, j) = \sum_{\ell=1}^{k} A(i, \ell) B(\ell, j)$

(iv) $A^t \in K^{k \times n}$ durch $A^t(i, j) = A(j, i)$

Beispiel II.1.4: Seien A und B wie in Beispiel 2.1.2 dann ist

$$AB = \begin{pmatrix} 10 & -2 \\ -3 & 3 \end{pmatrix} \text{ und } BA = \begin{pmatrix} 1 & 4 & 1 \\ 0 & 1 & -1 \\ 3 & 4 & 11 \end{pmatrix}$$

Ist jetzt noch zusätzlich

$$C = \begin{pmatrix} 1 & 2 & 0 \\ 0 & -1 & 0 \\ 2 & 2 & 1 \end{pmatrix} \in \mathbb{R}^{3 \times 3}$$

gegeben, so ist $AC = \begin{pmatrix} 7 & 6 & 3 \\ -2 & -3 & -1 \end{pmatrix}$ und BC ist nicht definiert.

Proposition II.1.5 (Rechenregeln): *Seien $\lambda \in \mathbb{K}$ und A, B und C jeweils Matrizen, sodass die folgenden Ausdrücke definiert sind, dann gilt*

(i) $A + B = B + A$

(ii) $A + (B + C) = (A + B) + C$

(iii) $A(BC) = A(BC)$

(iv) $A(B + C) = AB + AC$

(v) $(A + B)C = AC + BC$

(vi) $A(\lambda B) = (\lambda A)B = \lambda(AB)$

(vii) $(A + B)^t = A^t + B^t$

(viii) $(AB)^t = B^t A^t$

(ix) $I_n A = A = A I_m$

Definition II.1.6: Sei $A \in K^{n\times n}$, man sagt A ist invertierbar oder regulär, falls es $B \in K^{n\times n}$ gibt mit

$$AB = BA = I_n$$

Notiere $A^{-1} := B$
und $\mathrm{GL}_n(K) := \{A \in K^{n\times n} \ : \ \text{es gibt } B \in K^{n\times n} \text{ mit } AB = BA = I_n\}$.

Bemerke dass $\mathrm{GL}_n(K)$ mit der Matrizenmultiplikation eine nicht abelsche Gruppe bildet.

Beispiel II.1.7: Die Matrix $\begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} \in \mathbb{R}^{2\times 2}$ ist invertierbar, da

$$\begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1/2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1/2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$$

und es gilt

$$\begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1/2 \end{pmatrix}$$

Die Matrix $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in \mathbb{R}^{2\times 2}$ ist nicht invertierbar denn für alle $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{R}^{2\times 2}$ gilt

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

2. Lineare Gleichungssysteme

Definition II.2.1: Seien $n, m \in \mathbb{N}$

(i) Ein lineares Gleichungssystem über K mit n Gleichungen und m Unbekannten ist ein System

$$\begin{array}{ccccccc} a_{1,1}x_1 & + & \dots & + & a_{1,m}x_m & = & b_1 \\ & \vdots & & \vdots & & \vdots & \vdots \\ a_{n,1}x_1 & + & \dots & + & a_{n,m}x_m & = & b_n \end{array}$$

wobei $a_{1,1}, ..., a_{n,m}, b_1, ..., b_n \in K$.

(ii) Das lineare Gleichungssystem hat folgende schematische Beschreibung

$$\left(\begin{array}{ccc|c} a_{1,1} & \dots & a_{1,m} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{n,1} & \dots & a_{n,m} & b_n \end{array} \right)$$

Die Matrix $A = (a_{i,j})$ heißt Koeffizientenmatrix des Linearen Gleichungssystems, $b = (b_1, ..., b_n)^t$ heißt rechte Seite und die Matrix $(A \mid b)$ heißt erweiterte Koeffizientenmatrix.

(iii) Die Menge

$$\mathbb{L} := \mathbb{L}(A, b) := \{x = (x_1, ..., x_m)^t \in K^m : x \text{ löst das lineare Gleichungssystem}\}$$

heißt Lösungsmenge und $\mathbb{L}^h := \mathbb{L}(A, 0)$ heißt homogene Lösungsmenge.
Bemerke dass $x \in \mathbb{L}^h$ genau dann wenn $A \cdot x = b$ gilt.

Definition II.2.2 (Treppenform): Seien $n, m \in \mathbb{N}$ und $T = (t_{i,j}) \in K^{n \times m}$. Gibt es $r \in \mathbb{N}$ und natürliche Zahlen $1 \leq s_1 < s_2 < \ldots < s_r \leq m$, sodass

(i) Für alle $1 \leq i \leq r$ gilt $t_{i,s_i} = 1$,

(ii) Für alle $1 \leq i \leq r$ und $1 \leq j \leq s_i$ ist $t_{i,j} = 0$,

(iii) Für alle $1 \leq i \leq r$ und $k \in \{1, ..., n\} \backslash \{i\}$ ist $t_{k,s_i} = 0$,

(iv) Für $i \geq r + 1$ und $1 \leq j \leq m$ ist $t_{i,j} = 0$,

Dann hat T Treppenform dabei heißt r Rang von T.

Beispiel II.2.3: Die Matrix

$$\begin{pmatrix} 0 & 1 & 2 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in \mathbb{R}^{4\times 6}$$

hat Treppenform.

Definition II.2.4 (Elementare Zeilenumformungen): Sei $A \in K^{n\times m}, \alpha, \alpha_1, ..., \alpha_n \in \mathbb{R}$. Die elementaren Zeilenumformungen sind gegeben durch folgende auszuführende Operationen

(i) Addition des α-fachen der j-ten Zeile zur i-ten Zeile,

(ii) Vertauschung der i-ten und j-ten Zeile,

(iii) Multiplikation der i-ten Zeile mit $\alpha_i \neq 0$.

Bemerkung II.2.5: Die elementaren Zeilenumformungen ändern die Lösungsmenge nicht und enstehen durch die Linksmultiplikation mit folgenden Additions-, Vertauschungs- und Diagonalmatrizen

(i) $A^{\alpha}_{i,j} := I_n + \alpha E_{i,j}$

(ii) $V_{i,j} := I_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$

(iii) $\mathrm{diag}(\alpha_1, ..., \alpha_n) := \sum_{i=1}^{n} \alpha_i E_{i,i}$ Wobei die $E_{i,j}$ jeweils an der Stelle (i, j) eine 1 und sonst 0-en eingetragen hat.

Satz 3 (Gauß-Algorithmus): *Sei $A \in K^{n\times m}$, so lässt sich A mit elementaren Zeilenumformungen in Treppenform bringen, d. h. es gibt $C \in \mathrm{GL}_n(K)$, sodass CA in Treppenform ist.*

Proposition II.2.6: *Seien $n, m \in \mathbb{N}$ und $T = (t_{i,j}) \in K^{n\times m}$ eine Matrix in Treppenform.*

(i) *Sei $J := \{1, ..., n\}\backslash\{s_1, ..., s_r\}$. Für $j \in J$ löst*

$$F^{(j)} := e_j - \sum_{i=1}^{r} t_{i,j} e_{s_i}$$

das homogene lineare Gleichungssystem $Tx = 0$.

(ii) *Es gilt für die homogene Lösungsmenge $\mathbb{L}^h$*

$$\mathbb{L}^h = \mathrm{span}(\{F^{(j)} \,:\, j \in J\}) = \Big\{ \sum_{j\in J} \lambda_j F^{(j)} \,:\, \lambda_j \in K \Big\}$$

Proposition II.2.7: *Seien $n, m \in \mathbb{N}, A \in K^{n\times m}$ und $b \in K^n$ und sei $x^{(s)}$ eine spezielle Lösung des Linearen Gleichungssystems $Ax = b$, dann gilt für die Lösungsmenge von $Ax = b$, dass*

$$\mathbb{L} = x^{(s)} + \mathbb{L}^h$$

Proposition II.2.8: *Seien $n, m \in \mathbb{N}, A \in K^{n\times m}, b \in K^n$ Für das lineare Gleichungssystem $Ax = b$ gilt*

(i) *Das lineare Gleichungssystem ist genau dann lösbar, wenn* $\operatorname{Rang}(A) = \operatorname{Rang}(A \mid b)$ *gilt.*

(ii) *Ist das lineare Gleichungssystem lösbar, dann ist die Lösung eindeutig genau dann, wenn* $\operatorname{Rang}(A) = m$ *gilt.*

(iii) *Genau dann ist für alle $c \in K^n$ das lineare Gleichungssystem lösbar, wenn* $\operatorname{Rang}(A) = n$ *gilt.*

Proposition II.2.9: *Genau dann ist $A \in K^{n\times n}$ invertierbar, wenn* $\operatorname{Rang}(A) = n$ *gilt.*

Proposition II.2.10: *Ist $A \in K^{n\times n}$ invertierbar, so löst für alle $1 \leq i \leq n$ die i-te Spalte $A^{-1}e_i$ von A^{-1} das lineare Gleichungssystem $Ax = e_i$.*

Beispiel II.2.11: Gegeben sei die reelle Matrix

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

Bestimme nun A^{-1} durch simultanes lösen der linearen Gleichungssysteme $Ax = e_1, Ax = e_2, Ax = e_3$.

$$\left(\begin{array}{ccc|ccc} 1 & -2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ -1 & 2 & 1 & 0 & 0 & 1 \end{array}\right)$$

$$\overset{III+I}{\to} \left(\begin{array}{ccc|ccc} 1 & -2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right)$$

$$\overset{I+2\cdot II}{\to} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 2 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right)$$

Also ist A invertierbar mit

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

3. Vektorräume

Definition II.3.1 (Vektorraum): Sei V eine Menge zusammen mit Abbildungen

$$+ : V \times V \to V$$

$$\cdot : K \times V \to V$$

Falls gilt

(i) $(V, +)$ ist abelsche Gruppe,

(ii) Für alle $v \in V$ ist $1_K \cdot v = v$,

(iii) Für alle $\lambda_1, \lambda_2 \in K$ und $v \in V$ ist $(\lambda_1 + \lambda_2)v = \lambda_1 v + \lambda_2 v$,

(iv) Für alle $\lambda \in K$ und $v_1, v_2 \in V$ ist $\lambda(v_1 + v_2) = \lambda v_1 + \lambda v_2$,

(v) Für alle $\lambda_1, \lambda_2 \in K$ und $v \in V$ ist $\lambda_1(\lambda_2 v) = (\lambda_1 \lambda_2)v$,

so heißt V ein Vektorraum über K oder K-Vektorraum.

Beispiel II.3.2: $K^n := \{(x_1, ..., x_n)^t \ : \ x_1, ..., x_n \in K\}$ ist mit den Verknüpfungen für $(x_1, ..., x_n)^t, (y_1, ..., y_n)^t \in K^n, \lambda \in K$ erklärt durch

$$(x_1, ..., x_n)^t + (y_1, ..., y_n)^t = (x_1 + y_1, ..., x_n + y_n)^t$$

$$\lambda(x_1, ..., x_n)^t = (\lambda x_1, ..., \lambda x_n)^t$$

ein K-Vektorraum. Ausserdem ist $K^{n \times m}$ mit der Addition und skalaren Multiplikation von Matrizen ein K-Vektorraum.

Definition II.3.3 (Untervektorraum): Sei V ein K-Vektorraum und $U \subseteq V$. U heißt Untervektorraum falls gilt

(i) $0 \in U$

(ii) Für alle $u_1, u_2 \in U$ ist $u_1 + u_2 \in U$

(iii) Für alle $\lambda \in K$ und $u \in U$ ist $\lambda u \in U$

Bemerke dass $(U, + |_{U \times U}, \cdot |_{K \times U})$ selbst wieder ein K-Vektorraum ist.

Definition II.3.4 (Vektorraumhomomorphismus): Seien V und W Vektorräume über K. Eine Abbildung $\phi : V \to W$ heißt K-lineare Abbildung oder Vektorraumhomomorphismus, falls gilt

(i) Für alle $v_1, v_2 \in V$ ist $\phi(v_1 + v_2) = \phi(v_1) + \phi(v_2)$,

(ii) Für alle $\lambda \in K$ und $v \in V$ ist $\phi(\lambda v) = \lambda\phi(v)$.

Ist K aus dem Kontext klar, so sagen wir häufig nur lineare Abbildung zu dieser Abbildung.

Es bezeichne weiterhin

$$\mathrm{Hom}(V,W) := \mathrm{Hom}_K(V,W) := \{\phi : V \to W : \phi \text{ ist Vektorraumhomomorphismus}\}$$

Diese Menge ist mit punktweiser Addition und skalarer Multiplikation ein K-Vektorraum, genauer ist $\mathrm{Hom}(V,W) \subseteq \mathrm{Abb}(V,W)$ ein Untervektorraum. Definiere weiterhin

$$\mathrm{Kern}(\phi) := \{v \in V \ : \ \phi(v) = 0\} \subseteq V$$

$$\mathrm{Bild}(\phi) := \{\phi(v) \ : \ v \in V\} \subseteq W$$

Diese sind Untervektorräume von V respektive W. Ist ϕ bijektiv, so heißt ϕ Isomorphismus. Ist $V = W$, so heißt ϕ Endomorphismus. Ist ϕ ein Endomorphismus und ein Isomorphismus, so heißt ϕ Automorphismus. Gibt es einen Isomorphismus zwischen zwei K-Vektorräumen V und W, so heißen V und W isomorph, notiere dies durch $V \cong W$.

Bemerkung II.3.5: Eine lineare Abbildung ϕ zwischen zwei K-Vektorräumen V und W ist genau dann injektiv, wenn $\mathrm{Kern}(\phi) = \{0\}$ gilt.

Definition II.3.6 (Lineare Unabhängigkeit, Basis): Sei V ein K-Vektorraum und $M \subseteq V$

(i) M heißt linear unabhängig falls für alle $v_1, ..., v_n \in M$ und $\lambda_1, ..., \lambda_n \in K$ mit $\lambda_1 v_1 + ... + \lambda_n v_n = 0$ bereits $\lambda_1 = ... = \lambda_m = 0$ folgt. Falls dies nicht gilt, so heißt M linear Abhängig.

(ii) Definiere den Spann von M durch

$$\mathrm{span}(M) = \langle M \rangle = \Big\{ \sum_{i=1}^{n} \lambda_i v_i \ : \ \lambda_1, ..., \lambda_n \in K, v_1, ..., v_n \in M \Big\}$$

Es gilt dass $\mathrm{span}(M) \subseteq V$ ein Untervektorraum ist.

(iii) $B \subseteq V$ heißt Basis falls B, linear unabhängig ist und $\mathrm{span}(B) = V$ gilt.

Proposition II.3.7: *Sei V ein K-Vektorraum und $B \subseteq V$. Folgende Aussagen sind äquivalent*

(i) *B ist eine Basis,*

(ii) *B ist minimales Erzeugendensystem, d. h. ist $C \subsetneq B$, dann ist* $\mathrm{span}(C) \subsetneq V$,

(iii) *B ist maximal linear unabhängige Teilmenge, d. h. ist $B \subsetneq C$, so ist C linear abhängig.*

Bemerkung II.3.8: Ist B eine Basis eines K-Vektorraums V so lässt sich jeder Vektor $v \in V$ als eindeutige Linearkombination der Basiselemente Schreiben.

Satz 4: *Mit dem Lemma von Zorn lässt sich beweisen, dass jeder Vektorraum eine Basis besitzt.*

Definition II.3.9 (Dimension): Sei V ein K-Vektorraum und B eine Basis von V. Dann hat jede weitere Basis von V genauso viele Elemente wie B. Wir definieren folglich den Begriff der Dimension von V durch

$$\dim(V) := \#B$$

Ist $\dim(V) < \infty$, so heißt V endlichdimensional.

Satz 5 (Basisergänzungssatz): *Sei V ein K-Vektorraum, dann gilt*

(i) *Jede linear unabhängige Teilmenge von V lässt sich zu einer Basis ergänzen.*

(ii) *Jedes Erzeugendensystem von V enthält eine Basis von V.*

Satz 6 (Fortsetzungssatz): *Seien V und W Vektorräume über K und B eine Basis von V*

(i) *Jede lineare Abbildung $\phi : V \to W$ ist eindeutig durch ihre Einschränkung $f := \phi\,|_B$ bestimmt.*

(ii) *Jede Abbildung $f : B \to W$ lässt sich auf eindeutige Weise zu einer linearen Abbildung $\phi : V \to W$ Fortsetzen mit $\phi\,|_B = f$.*

Definition II.3.10: Sei V ein endlichdimensionaler K-Vektorraum mit Basis $B = \{b_1, ..., b_n\}$. Dann definiert

$$D_B : V \to K^n \, , \; v = \sum_{i=1}^{n} \lambda_i b_i \mapsto (\lambda_1, ..., \lambda_n)^t$$

einen Vektorraumisomorphismus.

Satz 7 (Darstellungsmatrix): *Seien V und W Vektorräume über K mit geordneten Basen $B = (b_1, ..., b_m)$ respektive $C = (c_1, ..., c_n)$ und $\phi : V \to W$ linear. Dann gibt es genau eine Matrix $A \in K^{n\times m}$, sodass*

$$D_C \circ \phi = L_A \circ D_B$$

Das bedeutet, dass folgendes Diagramm kommutiert

$$\begin{tikzcd} V \arrow[r, "\phi"] \arrow[d, "D_B"'] & W \arrow[d, "D_C"] \\ K^m \arrow[r, "L_A"'] & K^n \end{tikzcd}$$

Dabei bezeichnet $L_A : K^m \to K^n$, $x \mapsto Ax$. Die Einträge der Matrix $A = (a_{i,j})$ sind eindeutig bestimmt durch

$$\phi(b_j) = \sum_{i=1}^{n} a_{i,j} c_i$$

Für $1 \leq j \leq m$. Notiere $D_{CB}(\phi) := A$.

Definition II.3.11: Sei V ein K-Vektorraum mit Basen B und C. Dann heißt

$$D_{CB} = D_{CB}(\mathrm{id})$$

Basiswechselmatrix.

Proposition II.3.12: *Seien V_1, V_2 und V_3 Vektorräume über K mit Basen B_1, B_2 und B_3 und $\phi : V_1 \to V_2$ und $\psi : V_2 \to V_3$ lineare Abbildungen. Seien zusätzlich C_1 eine weitere Basis von V_1 und C_2 eine weitere Basis von V_2. Dann gilt*

(i) $D_{B_2B_1}(\psi \circ \phi) = D_{B_3B_2}(\psi) D_{B_2B_1}(\phi)$,

(ii) $D^{-1}_{C_1B_1} = D_{B_1C_1}$,

(iii) $D_{C_2C_1}(\phi) = D_{C_2B_2} D_{B_2B_1}(\phi) D_{B_1C_1}$.

Definition II.3.13: Sei V ein K-Vektorraum und $U_1, ..., U_n \subseteq V$ Untervektorräume, dann ist

$$\sum_{i=1}^{n} U_i = \Big\{ \sum_{i=1}^{n} u_i \ : \ u_1 \in U_1, ..., u_n \in U_n \}$$

ein Untervektorraum. Gilt zusätzlich dass wenn $u_1 \in U_1, ..., u_n \in U_n$ mit $u_1 + ... + u_n = 0$ dass $U_1 = ... = u_n = 0$ Dann heißt die Summe $U_1 + ... + U_n$ direkt, schreibe in diesem Fall

$$\bigoplus_{i=1}^{n} U_i = \sum_{i=1}^{n} U_i$$

Definition II.3.14 (Faktorraum): Sei V ein K-Vektorraum und $U \subseteq V$ ein Untervektorraum. Definiere eine Äquivalenzrelation auf V durch

$$v_1 \sim v_2 :\Longleftrightarrow v_1 - v_2 \in U$$

Für die Äquivalenzklasse von $v \in V$ gilt

$$v + U := [v] = \{w \in V \,:\, v \sim w\}$$

und sei

$$V/U := \{[v] \,:\, v \in V\}$$

Auf V/U wird durch

$$[v] + [w] := [v + w]$$
$$\lambda[v] := [\lambda v]$$

eine Vektorraumstruktur erklärt, V/U heißt Quotientenvektorraum oder Faktorraum.

Satz 8 (Homomorphiesatz): *Seien V und W Vektorräume über K, $\phi : V \to W$ linear und U ein Untervektorraum mit $U \subseteq \operatorname{Kern}(\phi)$. Dann gibt es genau eine lineare Abbildung $\tilde{\phi} : V/U \to W$ mit $\tilde{\phi} \circ \pi = \phi$. Dass bedeutet das folgendes Diagramm kommutiert*

$$\begin{tikzcd} V \arrow[r, "\phi"] \arrow[d, "\pi"'] & W \\ V/U \arrow[ur, dashed, "\tilde{\phi}"'] & \end{tikzcd}$$

Ist $U = \operatorname{Kern}(\phi)$, so ist $\tilde{\phi}$ injektiv und es gilt $V/\operatorname{Kern}(\phi) \cong \operatorname{Bild}(\phi)$.

Satz 9 (Dimensionsformel): *Sei V ein K-Vektorraum mit $\dim(V) = n$.*

(i) *Ist $U \subseteq V$ ein Untervektorraum, dann ist $\dim(V/U) = \dim(V) - \dim(U)$.*

(ii) *Sind $U_1, U_2 \subseteq V$ Untervektorräume, so gilt*

$$\dim(U_2 + U_2) = \dim(U_1) + \dim(U_2) - \dim(U_1 \cap U_2)$$

(iii) *Ist W ein weiterer K-Vektorraum und $\phi : V \to W$ linear, so ist*

$$\dim(V) = \dim(\operatorname{Kern}(\phi)) + \dim(\operatorname{Bild}(\phi))$$

Definition II.3.15: Seien V und W Vektorräume über K und $\phi : V \to W$ linear. Dann heißt $\operatorname{Rang}(\phi) := \dim(\operatorname{Bild}(\phi))$ der Rang von ϕ. Seien $n, m \in \mathbb{N}$ und $A \in K^{n\times m}$. Dann heißt $\operatorname{Kern}(A) := \{x \in K^m \,:\, Ax = 0\}$ der Kern von A.

Kapitel III.

Endomorphismen von Vektorräumen

In diesem Kapitel wollen wir im ersten Teil uns Endomorphismen von Vektorräumen, welche uns vielerlei Eigenschaften und Kenngrößen (Invarianten) bieten werden, anschauen. Anwendungen finden diese Theorien zu genüge in der Mathematik und sind daher trotz ihrer Elementarität dennoch von hoher Bedeutung.

1. Determinante und deren Eigenschaften

Definition III.1.1: (Ähnlichkeit) Sei K ein Körper und seien $A, B \in K^{n \times n}$. Existiert eine Matrix $S \in \mathrm{Gl}_n(K)$ mit $A = SBS^{-1}$, so sagen wir, dass A und B ähnlich sind.

Bemerkung III.1.2: Wir interessieren uns nun im folgenden für *Ähnlichkeitsinvarianten*, d. h. wir suchen Größen, die bei zwei ähnlichen Matrizen gleich bleiben. Ein erstes Beispiel ist der Rang von Matrizen.

Weitere Invarianten sind gegeben durch die Determinante, Eigenwerte und die Spur, wobei alle drei in gewisser Weise zusammenhängen.[1]

[1]Andere Invarianten sind beispielsweise auch die Jordan-Normalform.

Definition III.1.3 (Leibniz-Definition der Determinanten): (i) Sei K ein Körper und sei $A = (\alpha_{i,j}) \in K^{n\times n}$ eine quadratische Matrix. Wir definieren

$$\det(A) = \sum_{\sigma\in S_n} \Big(\operatorname{sgn}(\sigma)\prod_{i=1}^{n} \alpha_{i,\sigma(i)}\Big)$$

(ii) Sei V ein endlich-dimensionaler K-Vektorraum und $\phi \in \operatorname{End}(V)$. Wir definieren die Determinante $\det(\phi)$ als die Determinante einer Darstellungsmatrix bzgl. einer gewählten Basis.[2]

Da wir jeden Endomorphismus $\phi \in \operatorname{End}(V)$ auf einem endlich dimensionalen K-Vektorraum als Matrix A auffassen können, sparen wir uns die Eigenschaften gesondert zu betrachten, da diese gleich sind.

Proposition III.1.4 (Grundlegende Eigenschaften): *Sei K ein Körper, $n \in \mathbb{N}$. Definiere $D : \prod_{i=1}^{n} K^n \to K$, $(x_1, \dots, x_n) \mapsto \det(x_1 \mid \dots \mid x_n)$.*

(i) *Die Abbildung ist in jedem Argument linear.*

(ii) *Die Abbildung ist alternierend, d. h. sind mindestens zwei Spalten gleich, so ist die Determinante 0.*
Für einen Körper mit $\operatorname{char}(K) \neq 2$ bedeutet dies, dass sich das Vorzeichen ändert, wenn man zwei Spalten vertauscht.

(iii) *Die Abbildung ist normiert, d. h. $D(e_1 \mid \dots \mid e_n) = 1$, wobei $(e_1, \dots, e_n)$ die kanonische Einheitsbasis des K^n ist.*

Bemerkung III.1.5 (Folgerungen aus der letzten Proposition):

(i) Die Determinante ist eindeutig bestimmt.

(ii) Wir können innerhalb der Determinantenfunktion Spalten- und Zeilenumformungen machen.
Es gilt mit der Notation von Definition II.2.4

$$\begin{aligned}
\det(A^{\alpha}_{i,j}A) &= \det(A)\\
\det(V_{i,j}A) &= -\det(A)\\
\det(\operatorname{diag}(\alpha_1,\dots,\alpha_n)A) &= \prod_{i=1}^{n}\alpha_i \det(A)
\end{aligned}$$

(iii) Enthält A eine Nullspalte so ist die Determinante 0.

[2] Wir werden sehen, dass die Wahl der Basis egal ist.

(iv) Als direkte Folgerung der letzten Punkte mit dem Gauß-Algorithmus bekommen wir

Eine Matrix A ist über K genau dann invertierbar, wenn $\det(A) \neq 0$.

Satz 10 (Wichtige Eigenschaften): *Seien K ein Körper,$n \in \mathbb{N}$ und $A, A_1, A_2 \in K^{n\times n}$.*

(i) *Es gilt* $\det(A) = \det(A^t)$.

(ii) *Es gilt* $\det(A_1 A_2) = \det(A_1)\det(A_2)$.

(iii) *Ist A invertierbar, dann gilt* $\det(A^{-1}) = \det(A)^{-1}$.

(iv) *Die Determinante ist eine Ähnlichkeitsinvariante, d. h. für $S \in \mathrm{Gl}_n(K)$ und gilt* $\det(SAS^{-1}) = \det(A)$.

Gerade der letzte Punkt dieses Satzes war Teil unseres Zieles eine Invariante von Endomorphismen kennenzulernen.

Satz 11 (Laplace-Entwicklung): *Es seien K Körper, $n \in \mathbb{N}$ und $A = (a_{i,j}) \in K^{n\times n}$. Ferner sei $k \in \{1, \dots, k\}$.*

(i) *Die Laplace-Entwicklung nach der $k-$ten Zeile ist*

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

(ii) *Die Laplace-Entwicklung nach der $k-$ten Zeile ist*

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

Hierbei bezeichnet $A_{k,j}$ die Matrix, die durch Streichen der $k-$ten Zeile und Streichen der $j-$ten Spalte entsteht („Streichungsmatrix“).

Bemerkung III.1.6 (Vorzeichen bei der Laplace-Entwicklung): Die Vorzeichen der jeweiligen Summanden kann man sich leicht merken mit dem „Schachbrettmuster“, so z. B. für eine 3×3 Matrix

$$\begin{pmatrix} + & - & + \\ - & + & - \\ + & - & + \end{pmatrix}$$

Bemerkung III.1.7 (Determinante Blockmatrix): Haben wir nun eine Blockmatrix der Form

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

gegeben (wobei A, B, C, D jeweils quadratische Matrizen sind), so gilt, wenn $C \neq 0$ und $B \neq 0$ nicht „$\det(M) = \det(AD) - \det(BC)$". Dies macht alleine deshalb keinen Sinn, da das Produkt AD nicht existieren muss.

Sollte $B = 0$ oder $C = 0$, so gilt aber

$$\det(M) = \det(A)\det(D)$$

Man findet diese Aussage auch unter dem Namen „Kästchensatz".

2. Eigenwerte und Eigenvektoren

Als nächstes interessieren wir uns für Eigenvektoren und Eigenwerte. Anschaulich gesprochen sind dies Vektoren, die unter einer linearen Abbildung ihre Richtung[3] beibehalten. Sie werden lediglich neuskaliert mit einem Skalar. Dies führt uns aber zu einer schönen Möglichkeit bestimmte Matrizen in die Form der Diagonalmatrix zu bringen. Dies wollen wir nun betrachten.

Definition III.2.1 (Eigenwert, Eigenvektor, Spektrum): Seien K ein Körper, V ein endlich-dimensionaler $K-$Vektorraum,$\phi \in \operatorname{End}(V)$.

(i) Sei $\lambda \in K$ für das ein $v \in V \backslash \{0\}$ existiert mit $\phi(v) = \lambda v$, dann heißt λ Eigenwert zum Eigenvektor v.

Analog definiere man dies für eine Matrix $A \in K^{n \times n}$.

(ii) Für einen Eigenwert λ nennen wir

$$\operatorname{Eig}(\phi, \lambda) = \{v \in V \mid \phi(v) = \lambda v\}$$

Eigenraum von ϕ zum Eigenwert λ.

(iii) Die Menge aller Eigenwerte von ϕ nennen wir Spektrum von ϕ

$$\begin{aligned} \operatorname{Spec}(\phi) &:= \{\lambda \in K \mid \lambda \text{ ist Eigenwert von } \phi\} \\ &= \{\lambda \in K \mid (\phi - \lambda \operatorname{id}_V) \text{ nicht bijektiv}\} \end{aligned}$$

[3]Richtung ist hierbei ein Konzept, welches wir auf Prähilberträumen haben.

Definition III.2.2 (Charakteristisches Polynom): Seien K ein Körper, V ein endlich dimensionaler $K-$Vektorraum,$\phi \in \mathrm{End}(V)$. Dann heißt

$$\chi_\phi(x) = \det(\phi - x\,\mathrm{id}_V)$$

das charakteristische Polynom von ϕ.

Bemerkung III.2.3 (Zusammenhang des char. Polynoms und der Eigenwerte): Die Nullstellen des charakteristischen Polynom sind gerade die Eigenwerte, sofern diese überhaupt existieren über dem jeweiligen Körper

Warum sind die Nullstellen aber gerade die Eigenwerte? Dies wollen wir uns schnell herleiten.

Sei $A \in K^{n\times n}$. Die Eigenwertgleichung lässt sich auch schreiben als

$$(A - \lambda I_n)v = \mathbf{0}.$$

Wir verlangen per Definition, dass $v \neq 0$, daher wollen wir $\lambda \in K$ finden, die dies erfüllen und das ist genau dann der Fall, wenn $(A - \lambda I_n)$ nicht vollen Rang hat, oder anders formuliert $\det((A - \lambda I_n)) = 0$.

Bemerkung III.2.4 (Eigenvektoren bestimmen): Wenn wir nun für eine Matrix $A \in K^{n\times n}$ zu einem Eigenwert λ den Eigenraum suchen wollen, müssen wir lediglich wie in der Definition bereits ersichtlich $\mathrm{Kern}(A - \lambda I_n)$ bestimmen.

Definition III.2.5 (Diagonalisierbarkeit): Sei alles wie in Definition III.2.1. .

Gibt es eine Basis B von V und $\lambda_1, \ldots, \lambda_n \in K$, sodass $D_{BB}(\phi) = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$, so heißt ϕ diagonalisierbar.

Im Falle einer Matrix und $\lambda_1, \ldots, \lambda_n \in K$ nennen wir $A \in K^{n\times n}$ genau dann diagonalisierbar, wenn $S \in \mathrm{Gl}_n(K)$ existiert mit $\mathrm{diag}(\lambda_1, \ldots, \lambda_n) = SAS^{-1}$.

Satz 12 („Hauptsatz" der Eigenwerttheorie): *Sei $A \in K^{n\times n}$ und sei* $\mathrm{Spec}(A) = \{\lambda_1, \ldots, \lambda_k\}$

(i) *Die Summe der Eigenräume ist direkt, d. h.*

$$\sum_{i=1}^{k} \mathrm{Eig}(A, \lambda_i) = \bigoplus_{i=1}^{k} \mathrm{Eig}(A, \lambda_i).$$

(ii) *Es gilt $k \leq n$, also gibt es höchstens n voneinander verschiedene Eigenwerte. Gibt es genau n verschiedene Eigenwerte über K, so ist A diagonalisierbar.*

(iii) *A ist genau dann diagonalisierbar, wenn*

$$K^n = \bigoplus_{i=1}^{k} \operatorname{Eig}(A, \lambda_i),$$

d. h. es gibt eine Basis aus Eigenvektoren von A.

Analog gelten die Aussagen für einen Endomorphismus ϕ eines endlichdimensionalen K-Vektorraums V.

Man könnte meinen, dass die Eigenwerte, Determinante und die Spur drei voneinander unabhängige Größen sind, dies wollen wir aber kurz widerlegen.

Bemerkung III.2.6 (Spur-Eigenwerte-Determinante): Sei $A = (a_{i,j}) \in K^{n\times n}$. Die Abbildung

$$\operatorname{Spur} : K^{n\times n} \to K,\ A \mapsto \sum_{i=1}^{n} a_{i,i}$$

heißt Spur. Diese Abbildung ist linear. Es handelt sich um eine weitere Invariante unter Basiswechsel, d. h. für $S \in \mathrm{Gl}_n(K)$ gilt $\operatorname{Spur}(SAS^{-1}) = \operatorname{Spur}(A)$.

Es gilt jetzt sofern alle Eigenwerte $\lambda_1, \dots, \lambda_n$ (Mehrfachzählung möglich, d. h. mit algebraischer Vielfachheit) über K existieren, dass

$$\operatorname{Spur}(A) = \sum_{i=1}^{n} \lambda_n,$$
$$\det(A) = \prod_{i=1}^{n} \lambda_n.$$