Inhalte der Vorlesung „Lineare Algebra I“

Im folgenden finden Sie eine Kurzbeschreibung der Inhalte und Ergebnisse der Vorlesung „Lineare Algebra I“ im WS 1998/99, die von Uwe Nagel gehalten wurde.

I. Matrizenrechnung

1. Ringe und Körper Ein Ring $(R, +, \cdot)$ ist eine Menge R mit einer Addition $+$ und einer Multiplikation $\cdot$, so daß $(R, +)$ eine abelsche Gruppe ist, die Multiplikation assoziativ ist und die Distributivgesetze gelten. Ein Körper ist ein Ring K, so daß $(K \setminus \{0_K\}, \cdot)$ eine abelsche Gruppe ist.

2. Matrizen Es sei R ein Ring, und es seien m, n natürliche Zahlen. Für geeignete Matrizen über R ist eine Addition und eine Multiplikation erklärt, so daß gilt: Die Menge $K^{m,n}$ der $m \times n$ Matrizen über einem Körper K bildet zusammen mit der Matrizenaddition und der Multiplikation mit Skalaren einen K-Vektorraum. Die Menge $R^{n,n}$ bildet zusammen mit der Matrizenaddition und -multiplikation einen Ring, der i.a. nicht kommutativ ist. Er enthält eine Eins genau dann, wenn R ein Ring mit Eins ist. Sind $A, B \in R^{n,n}$ invertierbar, so ist auch das Produkt $A \cdot B$ invertierbar, und es gilt $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$. Daher ist über einem Ring R mit Eins die Menge der invertierbaren Matrizen aus $R^{n,n}$ mit der Matrizenmultiplikation eine Gruppe. Ist $A \in R^{m,n}$, so ist die Transponierte A^t ein Element von $R^{n,m}$. Die Transponierte und die Inverse einer Elementarmatrix sind wieder Elementarmatrizen.

3. Treppennormalform und Rang einer Matrix Es sei K ein Körper. Zu jeder Matrix $A \in K^{m,n}$ gibt es genau eine Matrix T in Treppennormalform, so daß für eine geeignete invertierbare Matrix $P \in K^{m,m}$ gilt: $A = P \cdot T$. Die Matrix T heißt die Treppennormalform von A. Mit ihrer Hilfe werden die charakteristischen Spaltenindizes und der Rang von A definiert. Die Treppennormalform wird mit dem Gauß-Algorithmus berechnet. Der Rang eines Produktes von Matrizen ist nicht größer als der Rang jedes Faktors. Der Rang ändert sich nicht bei einer Multiplikation mit einer invertierbaren Matrix und beim Transponieren. Eine Matrix A hat den Rang r genau dann, wenn es invertierbare Matrizen P, Q gibt, so daß gilt: $A = P \cdot (\sum_{i=1}^{r} E_{ii}) \cdot Q$. Für eine quadratische Matrix $A \in K^{n,n}$ sind äquivalent: (a) A ist invertierbar; (b) A ist Produkt von Elementarmatrizen; (c) Es gibt eine Matrix $B \in K^{n,n}$ mit $A \cdot B = E_n$; (d) $\mathrm{Rg}(A) = n$.

4. Lineare Gleichungssysteme Es sei $A \cdot x = b$ ein lineares Gleichungssystem über dem Körper K mit erweiterter Koeffizientenmatrix $A' = (A\ b) \in K^{m,n+1}$. Dann besitzt dieses (mindestens) eine Lösung genau dann, wenn gilt: $\mathrm{Rg}(A) = \mathrm{Rg}(A')$. Die Menge $\mathcal{H}$ der Lösungen des homogenen Gleichungssystems $A \cdot x = 0$ ist ein K-Vektorraum der Dimension $n - \mathrm{Rg}(A)$. Insbesondere hat das homogene Gleichungssystem $A \cdot x = 0$ nur die triviale Lösung $(0, \ldots, 0)^t$ genau dann, wenn A den Rang n hat. Ist l eine Lösung von $A \cdot x = b$, so ist $l + \mathcal{H}$ die Menge aller Lösungen von $A \cdot x = b$. Diese kann man berechnen, indem man mit Hilfe des Gauß-Algorithmus die Treppennormalform der erweiterten Koeffizientenmatrix A' bestimmt und dann in geeigneter Weise „(-1)-Zeilen“ einfügt.

5. Determinanten von Matrizen Es sei R ein kommutativer Ring mit Eins. Für $A \in R^{n,n}$ ist dann nach Leibniz die Determinante von A definiert. Aus der Definition ergeben sich Regeln zur Änderung der Determinante bei Multiplikation mit einer Elementarmatrix. Diese erlauben auch eine axiomatische Definition der Determinante. Wichtige Ergebnisse sind der Determinantenmultiplikationssatz und die Formel $A \cdot \mathrm{adj}\, A = \mathrm{adj}\, A \cdot A = \det(A) \cdot E_n$. Letztere impliziert den Entwicklungssatz von Laplace und die Cramersche

Regel. Zur Berechnung der Determinante einer Matrix über einem Körper benutzt man meist den Gauß-Algorithmus.

6. Eine Anwendung in der Kryptologie Für jede ganze Zahl $n > 1$ ist $\mathbb{Z}/n\mathbb{Z}$ ein kommutativer Ring mit Eins. Er ist ein Körper genau dann, wenn n eine Primzahl ist. Ein Element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ ist invertierbar genau dann, wenn a und n teilerfremd sind. Das Inverse berechnet man mit Hilfe des Euklidischen Algorithmus'. Eine Geheimschrift läßt sich mit einer Chiffriermatrix konstruieren. Ihre Inverse berechnet man mit Hilfe der Adjunkte.

II. Algebraische Grundbegriffe

1. Mengen und Abbildungen Eine Menge ist eine „Zusammenfassung von Gegenständen." Mengen werden durch Abbildungen zueinander in Beziehung gesetzt. Eine Abbildung $f : M \to N$ besteht aus dem Definitionsbereich M, dem Wertebereich N und der Zuordungsvorschrift f. Sie ist surjektiv, wenn jedes Element $n \in N$ (mindestens) ein Urbild hat, und sie ist injektiv, wenn jedes Element $n \in N$ höchstens ein Urbild hat. Ist f bijektiv, so gibt es genau eine Umkehrabbildung. Die Komposition von Abbildungen ist assoziativ. Sind f und g injektive Abbildungen, so ist auch $f \circ g$ injektiv. Dies bleibt auch richtig, wenn man „injektiv" durch „surjektiv" oder „bijektiv" ersetzt.

2. Gruppen Eine Gruppe ist eine Menge G mit einer assoziativen Verknüpfung, so daß es ein neutrales Element gibt und jedes Element von G ein Inverses hat. Eine Teilmenge von G ist eine Untergruppe, wenn sie mit der von G induzierten Verknüpfung eine Gruppe ist. Dies läßt sich mit dem Untergruppenkriterium entscheiden. Ein Gruppenhomomorphismus $\varphi : G \to H$ ist eine Abbildung zwischen Gruppen G und H, die strukturverträglich ist. Ist φ noch bijektiv, so wird φ Isomorphismus genannt. Die Determinantenabbildung $A \mapsto \det A$ liefert nach dem Determinantenmultiplikationssatz einen Homomorphismus $(\mathrm{Gl}_n(K), \cdot) \to (K \setminus \{0\}, \cdot)$.

3. Ringe Ein Ringhomomorphismus ist eine strukturverträgliche Abbildung zwischen Ringen. Ist diese bijektiv, so spricht man von einem Isomorphismus von Ringen. Die Restklassenabbildung $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, a \mapsto \overline{a}$, ist ein Ringhomomorphismus. Ist R ein Ring mit Eins, so ist der Polynomring $R[X]$ ein Ring mit Eins. Zwei Polynome sind genau dann gleich, wenn ihre Koeffizienten übereinstimmen. Jedes vom Nullpolynom verschiedene Polynom hat einen Grad. Über einem Körper K gilt für $f, g \neq 0$ in $K[X]$: $\deg f \cdot g = \deg f + \deg g$.

4. Körper Ist K ein Körper, so ist $a \cdot b \neq 0$ für alle Elemente $a, b \neq 0$ in K. Mit Hilfe der reellen Zahlen kann man den Körper der komplexen Zahlen konstruieren.

III. Vektorräume

1. Unterräume und Erzeugendensysteme Es sei K ein Körper. Ein K-Vektorraum V ist eine Menge mit einer Addition $V \times V \to V$ und einer Skalarmultiplikation $K \times V \to V$, so daß V zusammen mit der Addition eine abelsche Gruppe bildet und Addition und Skalarmultiplikation miteinander verträglich sind. Wichtige Beispiele sind der Vektorraum $K^{m,n}$ der $m \times n$ Matrizen und der Polynomring $K[X]$. Ferner kann man für jede Menge M und jeden K-Vektorraum V die Menge $\mathrm{Abb}(M, V)$ aller Abbildungen $M \to V$ zu einem K-Vektorraum machen. Ein Unterraum des K-Vektorraums V ist eine Teilmenge, die mit der von V induzierten Addition und Skalarmultiplikation einen K-Vektorraum bildet. Eine Linearkombination von Vektoren $v_1, \ldots, v_n \in V$ ist ein Element $\sum_{i=1}^{n} \lambda_i v_i \in V$, wobei die λ_i Skalare, also Elemente von K, sind. Ist E eine Teilmenge von V, so bildet die Menge aller Linearkombination von endlich vielen Elementen von E einen Unterraum

$\langle E \rangle$ von V, der der von E erzeugte Unterraum heißt. E heißt ein Erzeugendensystem von V, wenn $\langle E \rangle = V$ ist. Besitzt V ein endliches Erzeugendensystem, so nennt man V einen endlich erzeugten Vektorraum.

2. Lineare Abbildungen Eine lineare, genauer K-lineare, Abbildung ist eine strukturverträgliche Abbildung zwischen K-Vektorräumen. Sie ist ein Isomorphismus, wenn sie bijektiv ist. Die Umkehrabbildung ist dann auch ein Isomorphismus. Die Komposition linearer Abbildungen ist linear. Die Menge $\mathrm{Hom}(V, W)$ der linearen Abbildungen vom Vektorraum V in den Vektorraum W ist ein Unterraum von $\mathrm{Abb}(V, W)$. Kern und Bild linearer Abbildungen sind Vektorräume. Eine lineare Abbildung ist injektiv genau dann, wenn ihr Kern trivial ist, d.h. nur aus dem Nullvektor besteht. Jede lineare Abbildung $\varphi : K^n \to K^m$ kann durch ihre kanonische Matrix beschrieben werden. Dies liefert einen Isomorphismus $\mathrm{Hom}(K^n, K^m) \to K^{m,n}$ und gestattet die Anwendung der Ergebnisse über lineare Gleichungssysteme auf das Studium von φ. Insbesondere ist die Abbildung φ ein Isomorphismus genau dann, wenn $m = n$ ist und ihre kanonische Matrix invertierbar ist. Die kanonische Matrix der Komposition von linearen Abbildungen ist das Produkt der einzelnen kanonischen Matrizen.

3. Dimension und Basen von Vektorräumen Es sei V ein K-Vektorraum. Vektoren $v_1, \dots, v_n \in V$ heißen linear unabhängig, wenn aus $\sum_{i=1}^n \lambda_i v_i = 0_V \quad \text{mit } \lambda_i \in K$ immer $\lambda_1 = \dots = \lambda_n = 0_K$ folgt. Eine Teilmenge E von V heißt linear unabhängig, wenn jede Auswahl von endlich vielen, paarweise verschiedenen Vektoren aus E linear unabhängig ist. Eine Basis von V ist ein linear unabhängiges Erzeugendensystem. Ist $E = \{v_1, \dots, v_n\}$ eine Teilmenge von V, so ist die Abbildung

$$\psi_E : K^n \longrightarrow V,\ (a_1, \dots, a_n)^t \mapsto \sum_{i=1}^n a_i v_i$$

linear. ψ_E ist surjektiv genau dann, wenn E ein Erzeugendensystem von V ist. ψ_E ist injektiv genau dann, wenn die Vektoren $v_1, \dots, v_n$ linear unabhängig sind. ψ_E ist ein Isomorphismus genau dann, wenn E eine Basis mit n Elementen ist. ψ_E heißt dann der Koordinatenisomorphismus zur Basis E. Das Urbild von $v \in V$ unter ψ_E ist der Koordinatenvektor von v bezüglich der Basis E. Hat V ein endliches Erzeugensystem E, so kann nach dem Basisergänzungssatz jede endliche, linear unabhängige Teilmenge von V durch Hinzunahme von Vektoren aus E zu einer Basis von V ergänzt werden. Jeder Unterraum eines endlich erzeugten Vektorraums V ist endlich erzeugt, die Basen von V haben dieselbe Anzahl von Elementen. Daher kann man diese Anzahl als Dimension von V definieren. Vermöge des Koordinatenisomorphismus ergibt sich die Klassifikation von endlich erzeugten Verktorräumen: Ist V endlich erzeugt, so ist V isomorph zu $K^{\dim V}$. Hat V die Dimension n, so ist eine Teilmenge E von V mit n Elementen ein Erzeugensystem von V genau dann, wenn sie eine Basis von V ist. Es gilt: $\dim K^{m,n} = m \cdot n$, $\dim_K K[X] = \infty$, $\dim_{\mathbb{R}} \mathbb{C} = 2$, $\dim_{\mathbb{Q}} \mathbb{R} = \infty$. Ist $A \in K^{m,n}$, so gilt für die lineare Abbildung $\varphi_A : K^n \to K^m, x \mapsto A \cdot x$: $\dim(\operatorname{im} \varphi_A) = \operatorname{Rg} A$ und $\dim(\ker \varphi_A) = n - \operatorname{Rg} A$. Der Gauß-Algorithmus liefert Verfahren zur Bestimmung einer Basis von $\operatorname{im} \varphi_A$ bzw. $\ker \varphi_A$ und zur Auswahl einer Basis aus einem Erzeugensystem. Für Unterräume U_1, U_2 von V mit endlicher Dimension gilt die Dimensionsformel

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

Die 1-dimensionalen Unterräume von $\mathbb{R}^3$ entsprechen den Geraden durch den Nullpunkt, die 2-dimensionalen Unterräume von $\mathbb{R}^3$ entsprechen den Ebenen durch den Nullpunkt.

4. Koordinatenmatrizen und Rang einer linearen Abbildung Lineare Abbildungen kann man durch „Übergang zu Koordinaten“ studieren: Ist V ein Vektorraum mit einer Basis B aus $n = \dim V$ Elementen und W ein Vektorraum mit einer Basis C aus $m = \dim W$ Elementen sowie $\varphi : V \to W$ eine lineare Abbildung, so hat man ein kommutatives Diagramm

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & W \\ \uparrow\psi_B & & \uparrow\psi_C \\ K^n & \xrightarrow{\varphi^{B,C}} & K^m, \end{array}$$

in dem die vertikalen Abbildungen die entsprechenden Koordinatenisomorphismen sind. Diese induzieren Isomorphismen $\ker\varphi \cong \ker\varphi^{B,C}$ und $\operatorname{im}\varphi \cong \operatorname{im}\varphi^{B,C}$. Insbesondere ist φ injektiv bzw. surjektiv genau dann, wenn $\varphi^{B,C}$ die entsprechende Eigenschaft hat. Mit Hilfe der Ergebnisse über $\varphi^{B,C}$ folgt: (a) Ist φ surjektiv, so ist $\dim V \geq \dim W$; (b) Ist φ injektiv, so ist $\dim V \leq \dim W$; (c) Ist $\dim V = \dim W$, so ist φ ein Isomorphismus genau dann, wenn φ injektiv oder surjektiv ist. Die kanonische Matrix von $\varphi^{B,C}$ heißt die Koordinatenmatrix von φ bezüglich der Basen B und C. Ihre i-te Spalte ist der Koordinatenvektor des Bildes des i-ten Basisvektors von B unter φ. Die Konstruktion liefert einen Isomorphismus $\operatorname{Hom}(V,W) \to K^{m,n}$, der von der Wahl der Basen B und C abhängt. Ist $V = W$, so ist die Koordinatenmatrix der identischen Abbildung die Übergangsmatrix für den Basiswechsel von B nach C. Sind B' und C' weitere Basen von V bzw. W, so gilt für die Koordinatenmatrizen $M_\varphi^{B',C'} = M_{id_W}^{C',C} \cdot M_\varphi^{B,C} \cdot (M_{id_V}^{B,B'})^{-1}$. Der Rang von φ ist als Dimension von $\operatorname{im}\varphi$ definiert. Nach dem Rangsatz ist er gleich dem Rang jeder Koordinatenmatrix von φ, und es gilt $\dim(\ker\varphi) = \dim V - \operatorname{Rg}\varphi$. Durch geeignete Wahl der Basen B und C kann man erreichen, daß die Koordinatenmatrix die einfache Gestalt $M_\varphi^{B,C} = \sum\limits_{i=1}^{\operatorname{Rg}\varphi} E_{ii}$ hat. Dies kann man als Klassifikation solcher linearer Abbildungen auffassen. Ist W ein beliebiger Vektorraum, so gilt immer noch das Prinzip der linearen Fortsetzung, d.h., ist B eine Basis von V, so gibt es genau eine lineare Abbildung $V \to W$, die eine gegebene Abbildung $B \to W$ fortsetzt.

5. Dualität Es sei V ein Vektorraum endlicher Dimension. Der Vektorraum V^* der Linearformen von V heißt Dualraum von V. Nach Wahl einer Basis B von V kann man einen Isomorphismus $V \to V^*$ mit Hilfe der dualen Basis von B explizit angeben. Hingegen gibt es einen kanonischen Isomorphismus $\delta : V \to V^{**}$, der ohne Kenntnis einer Basis von V beschrieben werden kann. Der Annulator N^0 einer Teilmenge N von V ist ein Unterraum von V^*. Es gilt $N^0 = (\langle N \rangle)^0$ und $\dim N^0 = \dim V - \dim\langle N \rangle$. Für Unterräume U, U_1, U_2 von V gilt $\delta(U) = U^{00}$ und $\delta(U_1 \cap U_2) = (U_1^0 + U_2^0)^0$. Die letzte Formel begründet einen Algorithmus zur Bestimmung einer Basis von $U_1 \cap U_2$. Ist $\varphi : V \to W$ eine lineare Abbildung zwischen den Vektorräumen endlicher Dimension V und W mit Basen B bzw. C, so ist die Koordinatenmatrix der dualen Abbildung $\varphi^* : W^* \to V^*$ bezüglich der dualen Basen von C bzw. B gerade die Transponierte der Koordinatenmatrix von φ bezüglich B und C, also $M_{\varphi*}^{C^*,B^*} = (M_\varphi^{B,C})^t$. Es gilt $(\operatorname{im}\varphi)^0 = \ker(\varphi^*)$.

6. Direkte Summen von Unterräumen Ist V ein Vektorraum endlicher Dimension mit Unterräumen $U_1, \ldots, U_s$, so ist V die direkte Summe von $U_1, \ldots, U_s$ genau dann, wenn jedes $v \in V$ eine eindeutige Darstellung $v = \sum\limits_{i=1}^{s} u_i$ mit $u_i \in U_i$ besitzt. Dies ist genau dann der Fall, wenn gilt: $V = U_1 + \ldots + U_s$ und $\dim V = \sum\limits_{i=1}^{s} \dim U_i$. Jeder Unterraum von V besitzt ein Komplement. Für eine lineare Abbildung $\varphi : V \to V$ ist $V = \ker\varphi \oplus \operatorname{im}\varphi$ genau dann, wenn $\ker\varphi \cap \operatorname{im}\varphi = \{0_V\}$ ist. Dies ist z.B. für Projektionen richtig.