Lineare Algebra II

Inoffizieller Mitschrieb

Stand: 19. April 2018

Vorlesung gehalten von:

Prof. Dr. Amador Martín-Pizarro
Abteilung für Angewandte Mathematik
Albert-Ludwigs-Universität Freiburg

0. Recap

Definition 0.1 – Ring

Ein (kommutativer) Ring (mit Einselement) ist eine Menge zusammen mit zwei binären Operationen $+, \cdot$, derart, dass:

- $(R, +)$ ist eine abelsche Gruppe
- $(R, \cdot)$ ist eine kommutative Halbgruppe
- die Dsitributivgesetze:
  $a(x + y) = ax + ay$
  $(x + y)z = xz + yz)$

Definition 0.2 – Integritätsbereich

Ein Integritätsbereich ist ein Ring ohne Nullteiler. Also $\forall x, y \in R : x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$

Definition 0.3 – Körper

Ein Körper ist ein Ring der Art, dass

1. $1 \neq 0$
2. $\forall x \in K : x \neq 0 \Rightarrow \exists x^{-1} : xx^{-1} = x^{-1}x = 1$

Bemerkung: Körper sind Integritätsbereiche.

Definition 0.4 – Charakteristik

Sei R ein nicht trivialer Ring $(0 \neq 1)$. $\varphi : \mathbb{Z} \to R, z \mapsto \begin{cases} \sum_{i=1}^{n} 1 & n >= 0 \\ -\sum_{i=1}^{n} 1 & \text{ansonsten} \end{cases}$
Dann ist φ ein Ringhomomorphismus.
Für den Kern von φ $(\mathrm{Ker}(\varphi))$ gibt es zwei Möglichkeiten.

1. $\mathrm{Ker}(\varphi) = \{0\}, p = 0$
2. $\mathrm{Ker}(\varphi) \neq \{0\}$. Dann gibt es ein kleinstes echt positives Element $p \in \mathrm{Ker}(\varphi)$.

R hat dann Charakteristik p ($\mathrm{Char}(R) = p$). Falls R ein Integritaetsbereich ist, dann ist p eine Primzahl.
Beispiele:
$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \dots, \bar{n}\}$ hat Charakteristik n.
Insbesondere enthält jeder Körper mit Charakteristik p eine "Kopie" von $\mathbb{Z}/m\mathbb{Z}$:
k hat Charakteristik p $\Rightarrow \mathbb{Z}/p\mathbb{Z} \overset{injectiv}{\leftrightarrow} K$.
Hier ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper:
$a \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\} \Rightarrow$ es ist a mit p teilerfremd. $1 = a \cdot b + p \cdot m \Rightarrow \bar{1} = \bar{a} \cdot \bar{b}$.

Definition 0.5 – Polynomring

Sei K ein Körper. Der Polynomring $K[T]$ in einer Variable R über K ist die Menge formeller Summen der Form:
$f = \sum_{i=0}^{n} a_i \cdot T^i, n \in \mathbb{N}$

Der Grad von $f \in K[T]$ ist definiert als:
Grad$(f) := max(m|m < n \wedge a_m \neq 0)$
Grad$(0) := -1$
Falls $Grad(f) = n$ und $n = 1$ heißt das Polynom normiert.
Die Summe und das Produkt von Polynomen sind definiert als:
$\sum_{i=0}^{n} a_i T^i + \sum_{j=0}^{m} b_j T^j := \sum_{k=0}^{max(m,n)} (a_k b_k) T^k$
$\sum_{i=0}^{n} a_i T^i \cdot \sum_{j=0}^{m} b_j T^j := \sum_{k=0}^{m+j} = c_K T^k, c_k = \sum_i +j = k a_i b_j$

Bemerkung: $K[T]$ ist ein Integritätsbereich.

Korollar 0.6

Es seien f, g beide $\neq 0$
$\Rightarrow$ Grad$(f \cdot g) =$ Grad$(f) +$ Grad$(g) \Rightarrow f \cdot g \neq 0$
Grad$(f + g) \leq max($Grad$(f),$ Grad$(g))$

Satz 0.7 – Division mit Rest

Gegeben $f, g \in K[T],$ Grad$(g) > 0$. Dann existieren eindeutige Polynome q, r, so dass $f = g\dot{q} + r$, wobei Grad$(r) <$ Grad(g).

Beweis: Eindeutigkeit: Angenommen $f = g \cdot q + r = g \cdot q' + r', q \neq q' \vee r \neq r'$.
$\Rightarrow g(q-q') = r'-r \Rightarrow$ Grad$(r'-r) = max($Grad$(r'),$ Grad$(r)) <$ Grad$(g) =$ Grad$(g(q-q')) \Rightarrow$ Widerspruch
$\Rightarrow q = q' \Rightarrow r = r'$ Existenz: Induktion auf Grad(f)
Grad$(f) = 0 \Rightarrow f = g \cdot 0 + f$
Grad$(f) = n + 1$
Grad$(f) <$ Grad$(g) = m \Rightarrow f = g \cdot 0 + f$
OBdA. $n + 1 =$ Grad$(f) \geq$ Grad$(g) = m > 0$
$f = a_{n+1} \cdot T^{n+1} + \hat{f},$ Grad$(\hat{f}) \leq n, a_{n+1} \neq 0$
Sei $f' = f - b_m^{-1} a_{n+1} T^{n+1-m} \cdot g \Rightarrow$ Grad$(f') \leq n$ Ia: $f' = g \cdot q' + r',$ Grad$(r') <$ Grad(g)
$f' = f - b - b^{-1} a_{n+1} Tn + 1 - m \cdot g \Rightarrow f = g(b_n^{-1} a_{n+1} T^{n+1-m} + q') + r' \Rightarrow$ Grad$(r') <$ Grad(g) □

Definition 0.8 – Polynom Teilt

$f, g, q \in K[T]$, Grad$(g) > 0$
g teilt $f = g|_f \Leftrightarrow f = g \cdot q$

Definition 0.9 – Nullstellen von Polynomen

$f \in K[T]$ besizt eine Nullstelle $\lambda \in K$ gdw. $(T - \lambda)|_f \Leftrightarrow f(\lambda) = 0$.
f lässt sich dann schreiben als $f = (T - \lambda)q + r$.

Lemma 0.10

$f \in K[t], f \neq 0,$ Grad$(f) = n \Rightarrow$ f besitzt höchstens n Nullstellen in k.

Beweis:

$n = 0 \Rightarrow f = a_0, a_0 \neq 0$

$n > 0$ Falls f keine Nullstellen in K besitzt $\Rightarrow$ ok!

Sonst, sei $\lambda \in K$ eine Nullstelle von f. $f = (T - \lambda) \cdot g, \text{Grad}(g) = n - 1 < n$

I.A besitzt g höchstens n - 1 Nullstellen. Jede Nullstelle von f ist entweder λ oder eine Nullstelle von g. $\Rightarrow$ f hat höchstens n Nullstellen.

$\square$

Definition 0.11 – Vielfachheit einer Nullstelle

$f \in K[T], f \neq 0, \lambda \in K$ Nullstelle von f $\Rightarrow f = (T - \lambda)^{K_\lambda} \cdot g, g(\lambda \neq 0$. K_λ ist die Vielfacheit der Nullstelle λ in f.

Definition 0.12

Ein Körper heißt algebraisch abgeschlossen, falls jedes Polynom über K positiven Grades eine Nullstelle besitzt.

Beispiele Ist $\mathbb{R}$ algebraisch abgeschlossen? Nein: $T^2 + 1$.
Bem.: $\mathbb{C}$ ist algebraisch abgeschlossen.
Bemerkung: Jeder algebraisch abgeschlossene Körper muss unendlich sein. Sei $K = \{\lambda_1, \dots \lambda_n\}, f = (T - \lambda), \dots, (T - \lambda_n) + 1$.

Lemma 0.13

K ist genau dann algebraisch abgeschlossen, wenn jedes Polynom positiven Grades in lineare Faktoren zerfällt.
$f = T(\lambda_1) \dots (T - \lambda_n)$.

Beweis:

$\Leftarrow$ trivial

$\Rightarrow$ $\text{Grad}(f) = n > 0 \Rightarrow f = (T - \lambda_1) \cdot g, \text{Grad}(g) \leq n - 1 < n \overset{I.A.}{\Rightarrow} f = c(T - \lambda_1) \dots (T - \lambda_n)$

$\square$

Definition 0.14 – Vektorraum

Vektorraum V über K ist eine abelsche Gruppe $(V, +, 0_V)$ zusammen mit einer Verknüpfung $K \times V \to V$ $(\lambda, v) \mapsto \lambda v$ die die folgenden Bedingungen erfüllt:

1. $\lambda(v + w) = \lambda v + \lambda w$
2. $\lambda(\mu\Big(\Big)\Big) = (\lambda\mu)v$
3. $(\lambda + \mu)v = \lambda v + \mu v$
4. $1_k v = v$

Definition 0.15 – Untervektorraum

Ein Untervektorraum $U \subset V$ ist eine Untergruppe, welche unter der Skalarmultiplikation abgeschlossen ist.

Bemerkung: $\{U_i\}_{i\in I}$ Untervektorräume von V $\Rightarrow$ $\bigcap_{i\in I} U_i$ ist Untervektorraum. Insb. gebenen $M \subset V$ existiert span$(M) =< M >=$ der kleinste Unterraum von V, der M enthält.
span$(M) = \sum_{i=1}^{n} \lambda_i m_i,\ m_i \in M, \lambda_i \in K, n \in \mathbb{N}$
M ist ein Erzeugendensystem für span(M)
Außerdem gilt:
$\sum_{i\in I} U_i = \text{span}(\bigcup_{i\in I} U_i)$
$M_1 \subset M_2 \Rightarrow \text{span}(M_1) \subset \text{span}(M_2)$

Definition 0.16 – Lineare Unabhängigkeit

Sei V ein Vektorraum über K. Dann gilt $v_1, \dots v_n$ sind linear unabhängig falls $\forall \lambda_1, \dots, \lambda_n \in K : \sum \lambda_i v_i \Rightarrow \lambda_1 = \dots = \lambda_n = 0$ $M \subset V$ ist linear unabhängig, falls jede endliche Teilmenge von M linear unabhängig ist. Äquivalent dazu ist: M ist linear unabhängig, falls kein Element von M sich als Linearkombination der anderen schreiben lässt.

Definition 0.17 – Basis

Sei $B = \{v_1, \dots, v_n\}, v_i \in V$. Die folgenden Aussagen sind äquivalent und definieren eine Basis:

1. B ist ein lineare unabhängiges Erzeugendensystem von V
2. Jedes Element von V lässt sich eindeutig als Linearkombination der Elemente in B schreiben.
3. B ist ein minimales Erzeugendensystem.
4. B ist maximal lineare unabhängig.

Satz 0.18 – Basisergänzungssatz

Sei $M \subset V$ lineare unabhängig, dann gilt $\exists B \subset V$, und B ist eine Basis welche M entält. Insbesondere hat jeder Vektorraum eine Basis. "Je zwei Basen sind in Bijektion".

Definition 0.19 – Dimension

V ist endlichdimensional, falls V eine endliche Basis besitzt. Sonst ist V unendlichdimensional. Fall V endlichdimensional ist, ist die Dimension von V definert durch:
$dim(V) = |B|$ mit B beliebeige Basis.

Satz 0.20 – Basisauswahlsatz

Sei $M \subset V$ ein Erzeugendensystem von V, dann gilt $\exists B \subset M$ mit B ist eine Basis von V.

Lemma 0.21

Sei $U \subset V$ ein Unterraum, dann gilt $\dim(V) < \infty \Rightarrow \dim(U) < \infty$

Lemma 0.22

Die Dimension ist modular: $\dim(U_1 + U_2) + \dim(U_1 \cap U_2) = \dim(U_1) + \dim(U_2)$

Definition 0.23 – Direktes Produkt von Vektorräumen

$V = U_1 \oplus U_2 \Leftrightarrow V = U_1 + U_2 \wedge U_1 \cap U_2 = \{0\}$
$V = \oplus_{i\in I} U_i \Leftrightarrow V = \sum_{i\in I} U_i$ und die Familie ist transversal: $\{U_i\}_{i\in I} \rightarrow U_i \cap (\sum_{j\in I} U_j) = \{0\}$

Definition 0.24 – Komplementär

Sei $U \subset V$ ein Unterverktorraum, dann gilt $\exists \hat{U} \subset V : V = U \oplus \hat{U}$.
$\hat{U}$ heißt dann Komplementär zu U.

Beispiele

K^2 ist ein K-VR. $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ ist eine Basis.

$U = \text{span}(\begin{pmatrix} 1 \\ 0 \end{pmatrix})$. $K^2 = U \oplus \text{span}(\begin{pmatrix} 0 \\ 1 \end{pmatrix})$. $K^2 = U \oplus \text{span}(\begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

Definition 0.25 – Lineare Abbildungen

$F : V \to W$ ist linear, falls gilt: $F(\lambda v + \mu u) = \lambda F(v) + \mu F(u)$

Definition 0.26 – Kern und Bild

$\text{Ker}(F) = \{v \in V \ F(v) = 0\}$
$\text{Im}(F) = \{w \in W | \exists v \in V : F(V) = w\}$
$\text{Ker}(F)$ ist ein Untervektorraum von V, $\text{Im}(F)$ ist ein Untervektorraum von W.

Lemma 0.27

Falls B eine Basis von V ist, ist $F(B)$ ein Erzeugendensystem von $Im(F)$. F ist injektiv genau dann wenn $\text{Ker}(F) = \{0\}$.

Lemma 0.28

V endlichdimensional: $dim(V) = dim(Ker(F)) + dim(Im(F))$.
$V/Ker(f) \cong \text{Im}(F)$.

Bemerkung: V, W endlichdimensional, $\{v_1, \dots, v_n\}$ Basis von V $V \cong K^n$, $v_i \mapsto e_i$.

Definition 0.29 – Matrix

Sei $F : V \to W, dim(V) = n, dim(W) = m, \{v_1, \dots, v_n\}$ Basis von V, $\{w_1, \dots, w_n\}$ Basis von W.
$K^n \cong V \overset{F}{\to} W \cong K^m$. Dadurch wird durch F und die beiden Basen eine Abbildung von K^n nach K^m definiert. Diese Diese Abbildung kann durch eine Matrix A dargestellt werden.

$$\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \mapsto A\Big(\lambda_1, \vdots \lambda_n\Big)$$

$F(v_j) = \sum_{i=1}^m a_{ij} w_i$
$F(v_1), \dots, F(v_n)$

$$\begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix}$$ ist die mxn Matrix A.

Definition 0.30 – Rang einer Matrix

$Rg(A) = \text{dim(span(Spaltenvektoren))} = \text{dim(span(Zeilenvektoren))}$
$F : V \to W$ linear. $Rg(F) = Rg(A) = dim(\text{Im}(F))$, mit A eine beliebige darstellende Matrix von F.

Satz 0.31 – Normalform

Es seien V, W endlichdimensional. Dann existieren Basen $\{v_1, \dots v_n\}$ von V, $\{w_1, \dots, w_n\}$ von W, so dass die darstellende Matrix von F der Form $\begin{pmatrix} 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$ ist.

Beweis: Sei $U = \mathrm{Ker}(F)$ und $\{v_{r+1}, \dots, v_n\}$ eine Basis von U. Sei U' ein Komplement von U in V $\Rightarrow V = U \oplus U'$. Sei $\{v_1, \dots, v_r\}$ eine Basis von U'. $B = \{v_1, \dots v_n\}$ ist eine Basis von V. $\mathrm{Im}(F)$ hat $\{F(v_1), \dots, F(v_r)\}$ als Basis.
$\sum_{i=1}^n \lambda_i F(v_i) = 0 \Rightarrow F(\sum_{i=1}^n \lambda_i v_i) = 0 \Rightarrow \sum_{i=1}^n \lambda_i v_i) \in U \wedge \sum_{i=1}^n \lambda_i v_i) \in U' \Rightarrow \sum_{i=1}^n \lambda_i v_i) = 0 \Rightarrow \lambda_1 = \dots \lambda_n = 0$. Ergänze $\{F(v_1), \dots, F(v_r)\}$ zu einer Basis $B' = \{w_1, \dots, w_m\}$ von W. $F(v_1), \dots, F(v_r), F(v_{r+1}), \dots, F(v_n)$
$\begin{pmatrix} 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$ □

Definition 0.32 – Invertierbarkeit von Matrizen

$A \in M_{n\times n}(K)$ ist invertierbar, fall es eine Matrix $B \in M_{n\times n}(K)$ gibt, so dass $A \cdot B = B \cdot A = Id_n$. B wird dann als A^{-1} bezeichnet.
$GL(n,k) = Gl_n(K) = \{A \in M_{n\times n}(K)\text{invertierbar}\}$ ist eine Gruppe.
$A \in GL_k(n) \Leftrightarrow \mathrm{rg}(A) = n$ (Eine Matrix ist genau dann invertierbar, wenn sie regulär ist).

Bemerkung: Sei A regulär. Dann besitz ein Gleichungssystem der Form $A \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ die Eindeutige Lösung, $A^{-1} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$.
Bemerkung: A ist regulär genau dann wenn A sich durch elementare Zeilenoperationen in Id_n überführen lässt.
$E_{i,j}$ sei Die Matrix, die an der Stelle ij 1 ist, ansonsten 0.
Elementare Zeilenoperationen sind:
Multiplikation der Zeile i mit λ: $\mathrm{Id}_n + (\lambda - 1)E_{i,j}$.
Addieren von λ mal der iten Zeilten zur jten: $Id_n + \lambda E_{i,j}$.
Vertauschung der i-ten und j-ten Zeile: $Id_n - E_{ii} - E_{jj} + E_{j,i} + E_{i,j}$

Bemerkung: Das inverse einer Matrix lässt sich durch nutzen dieser elementaren Zeilenoperationen nach z.B. dem Gauß-Jordan Verfahren errechnen:
$\left(A \,\middle|\, Id_n \right) \overset{Zeilenoperationen}{\rightarrow} \left(Id_n \,\middle|\, A^{-1} \right)$
Die linke Hälfte der Ergebnis Matrix enthält dann A^{-1}, denn:
$B_m \dots B_2 B_1 A = Id_n \Rightarrow B_m \dots B_1 = A^{-1}$

Definition 0.33 – Übergangsmatrizen

Es sei $dim(V) = n$ und $\{v_1, \dots, v_n\}$, $\{v'_1, \dots, v'_n\}$ Basen von V. Weiterhin sei $F : V \to V, v_i \mapsto v'_i$. Dann gilt:

$v'_i = \sum_{ij} s_{ij} v_j$ und die darstellende Matrix S von F, $S = \begin{pmatrix} s_{11} & \dots & s_{1m} \\ \vdots & \ddots & \vdots \\ s_{n1} & \dots & s_{nm} \end{pmatrix}$ ist regulär.