

Plenarübung Lineare Algebra II

(Inhalts)-Wochen 06/07



Link zu diesen Folien

Das heutige Programm

- 1 Wochenüberblick
- 2 Wochenwiederholung in wenigen Folien:
 - 1 Polynome
 - 2 Moduln
 - 3 Algebren
- 3 Übersicht der Kombination bekannter Strukturen
- 4 Intuition zu Moduln
- 5 Sinn der Vektorraumkonzepte in Moduln
- 6 Genauerer Blick auf das Untermodulkriterium
- 7 Zusammenspiel der Modul- und Ringeigenschaften in Algebren
- 8 Beispiel zu Einsetzungsoperationen
- 9 Übersicht Faktorstrukturen

Wochenüberblick

Wochenwiederholung

Bemerkung 28.5

- $(R^{\mathbb{N}_0})_{00}$ ist eine „neutrale“ Formulierung des Polynomringes
- zwei Polynome sind gleich, wenn die Folgen übereinstimmen
- **konstante Polynome**
 $(\alpha_0, 0, 0, \dots)$
- **lineare Polynome**
 $(\alpha_0, \alpha_1, 0, 0, \dots)$
- $R[t]$ ist eine isomorphe Darstellung unter Verwendung der Variable t
- zwei Polynome sind gleich, wenn die Koeffizienten aller Potenzen von t übereinstimmen
- **konstante Polynome**
 $\alpha_0 t^0$
- **lineare Polynome**
 $\alpha_0 t^0 + \alpha_1 t^1$

Moduln über kommutativen Ringen

Definition 29.1

Es sei $(R, +, \cdot)$ ein kommutativer Ring. Ein **R -Modul** $(M, +, \cdot)$ hat

$$+ : M \times M \rightarrow M$$

$$\cdot : R \times M \rightarrow M$$

- 1 $(M, +)$ ist abelsche Gruppe
- 2 gemischtes Assoziativgesetz

$$(\alpha \cdot \beta) \cdot u = \alpha \cdot (\beta \cdot u)$$

gemischte Distributivgesetze

$$\alpha \cdot (u + v) = (\alpha \cdot u) + (\alpha \cdot v)$$

$$(\alpha + \beta) \cdot v = (\alpha \cdot v) + (\beta \cdot v)$$

Definition 11.1

Es sei $(K, +, \cdot)$ ein Körper. Ein **K -Vektorraum** $(V, +, \cdot)$ hat

$$+ : V \times V \rightarrow V$$

$$\cdot : K \times V \rightarrow V$$

- 1 $(V, +)$ ist abelsche Gruppe
- 2 gemischtes Assoziativgesetz

$$(\alpha \cdot \beta) \cdot u = \alpha \cdot (\beta \cdot u)$$

gemischte Distributivgesetze

$$\alpha \cdot (u + v) = (\alpha \cdot u) + (\alpha \cdot v)$$

$$(\alpha + \beta) \cdot v = (\alpha \cdot v) + (\beta \cdot v)$$

Moduln über kommutativen Ringen

Definition 29.1

Es sei $(R, +, \cdot)$ ein kommutativer Ring. Ein **R -Modul** $(M, +, \cdot)$ hat

$$+ : M \times M \rightarrow M$$

$$\cdot : R \times M \rightarrow M$$

- ③ M heißt **unitärer Modul**, wenn $1 \in R$ existiert und neutral bzgl. der S -Multiplikation \cdot ist

$$1 \cdot u = u$$

Definition 11.1

Es sei $(K, +, \cdot)$ ein Körper. Ein **K -Vektorraum** $(V, +, \cdot)$ hat

$$+ : V \times V \rightarrow V$$

$$\cdot : K \times V \rightarrow V$$

- ③ $1 \in K$ ist neutral bzgl. der S -Multiplikation \cdot

$$1 \cdot u = u$$

Definition 29.16

Es sei $(R, +, \cdot)$ ein kommutativer Ring.

- 1 Ein unitärer R -Modul $(M, +, \cdot)$ heißt **frei**, wenn es ein linear unabhängiges Erzeugendensystem (eine **Basis**) von M gibt.
- 2 Ein unitärer R -Modul $(M, +, \cdot)$ heißt **endlich frei**, wenn es ein endliches, linear unabhängiges Erzeugendensystem (eine endliche Basis) von M gibt.

Lemma 29.18

Es seien R ein kommutativer Ring, M ein R -Modul und $(v_i)_{i \in I}$ eine Basis von M . Dann gilt:

Jeder Vektor $v \in M$ lässt sich in eindeutiger Weise (bis auf Summanden mit Nullkoeffizienten) aus Basisvektoren linearkombinieren.

Definition 29.22

Es sei $(R, +, \cdot)$ ein komm. Ring. Eine **R -Algebra** $(A, +, \cdot, \star)$ erfüllt:

- 1 $(A, +, \cdot)$ ist ein R -Modul.
- 2 $(A, +, \star)$ ist ein Ring.
- 3 Die **Multiplikation** \star ist verträglich mit der S -Multiplikation:

$$(\alpha \cdot a) \star b = \alpha \cdot (a \star b) = a \star (\alpha \cdot b)$$

Einsetzungshomomorphismus

Definition 30.3

Es seien $(R, +, \cdot)$ ein kommutativer Ring mit Eins und $(A, +, \cdot, \star)$ eine unitäre R -Algebra mit Eins. Für $a \in A$ heißt die Abbildung

$$\text{ev}_a: R[t] \ni p \mapsto \text{ev}_a(p) := p(a) \in A$$

der **Einsetzungshomomorphismus zu a** .

Definition 30.8

Es seien $(R, +, \cdot)$ ein kommutativer Ring mit Eins und $(A, +, \cdot, \star)$ eine unitäre R -Algebra mit Eins. Für $p \in R[t]$ mit $p = \sum_{k=0}^n \alpha_k t^k$ heißt die Abbildung

$$p(\cdot): A \ni a \mapsto p(a) = \sum_{k=0}^n \alpha_k a^k \in A$$

die **durch p induzierte Polynomfunktion** auf der Algebra A .

Definition 31.9

Es seien K ein Körper und $p \in K[t]$. Das Element $\lambda \in K$ heißt eine **Nullstelle** oder **Wurzel von p in K** , wenn $p(\lambda) = 0$ gilt.

Satz 31.12

Es seien K ein Körper und $p \in K[t]$ ein Polynom, $p \neq 0$. Dann gilt:

- 1 Es existieren $s \in \mathbb{N}_0$, paarweise verschiedene Zahlen $\lambda_1, \dots, \lambda_s \in K$ sowie Exponenten $n_1, \dots, n_s \in \mathbb{N}$ und ein Polynom $q \in K[t]$ ohne Nullstelle in K , sodass gilt:

$$p = (t - \lambda_1)^{n_1} \cdots (t - \lambda_s)^{n_s} \cdot q$$

Weiter gilt $\deg(p) = n_1 + \cdots + n_s + \deg(q)$.

- 2 Die Nullstellen von p sind genau die Zahlen $\lambda_1, \dots, \lambda_s \in K$.

Übersicht

Übersicht - Kombination von Strukturen

Polynome $R[t]$

Gruppe
($G, +$)

Modul
($M, +, \cdot$)

Ring (Rng)
($R, +, \star$)

Unitärer Modul
($M, +, \cdot$)

Ring mit 1
($R, +, \star$)

Vektorraum
($V, +, \cdot$)

Körper
($K, +, \star$)

Algebra
($A, +, \cdot, \square$)

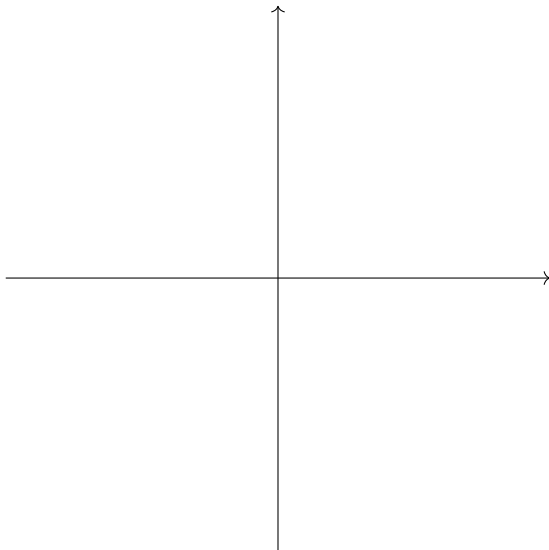
Unitäre Algebra
($A, +, \cdot, \square$)

Algebra mit 1
($A, +, \cdot, \square$)

Unitäre Algebra
mit 1 ($A, +, \cdot, \square$)

Moduln

Intuition zu Moduln



Vektorraumkonzepte in allgemeinen Moduln

- 1 Unterräume
- 2 Linearkombination
- 3 Erzeugendensysteme
- 4 Lineare (Un-)Abhängigkeit
- 5 Basen
- 6 Faktorräume
- 7 Darstellungsmatrizen
- 8 (Bi-)Dualräume

Charakterisierung der \mathbb{Z} -Moduln

Die \mathbb{Z} -Moduln sind gerade die abelschen Gruppen.

Ist $(G, +)$ eine abelsche Gruppe, dann ist $(G, +, \cdot)$ mit

$$z \cdot g := \underbrace{(g + \cdots + g)}_{z\text{-mal}} \quad (*)$$

ein \mathbb{Z} -Modul.

Ist $(M, +, \cdot)$ ein \mathbb{Z} -Modul, dann ist $(M, +)$ eine abelsche Gruppe und $(*)$ gilt.

Beispiel - Modulbasen verschiedener Kardinalitäten

Beispiel

Sei V ein K -Vektorraum mit Basis $(e_i)_{i \in \mathbb{N}}$ und $n \in \mathbb{N}$. Dann besitzt $\text{Endo}(V)$ aufgefasst als Modul über sich selbst eine n -elementige Basis.

Untermodulkriterium mit einem Skalar

Aufgabe

Es sei $(M, +, \cdot)$ ein R -Modul und $U \subseteq M$. Beweisen oder widerlegen Sie: U ist genau dann ein Untermodul von M , wenn U nichtleer ist und für alle $u, \bar{u} \in U$ und $\alpha, \beta \in R$ gilt, dass

$$\alpha u + \beta \bar{u} \in U.$$

Algebren

Beispiel einer Nicht-Algebra

\mathbb{C} als \mathbb{C} Vektorraum mit komponentenweiser Ringmultiplikation

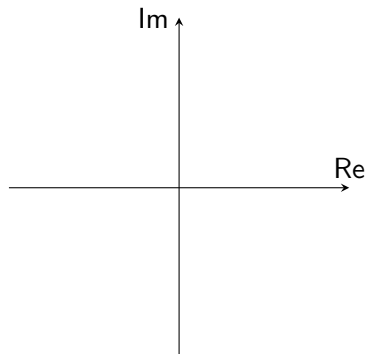
Wir betrachten

$$\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R}\}$$

$$+ : (a + bi, c + di) \mapsto (a + c) + (b + d)i$$

$$\cdot : (a + bi, c + di) \mapsto (ab - bd) + (ad + bc)i$$

$$\star : (a + bi, c + di) \mapsto (ac) + (bd)i$$



Zusammenspiel der Vektorraum- und Ringeigenschaften

Lemma:

Jede endlichdimensionale und nullteilerfreie K -Algebra $(A, +, \cdot, \star)$ mit Eins ist eine Divisionsalgebra.

Beweis:

Beispiel der zwei Einsetzungssichtweisen

Wie sehen die möglichen Einsetzungen von $\{t^k \mid k \in \llbracket 1, 5 \rrbracket\} \subseteq \mathbb{R}[t]$ und

$$\left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \right\} \subseteq \mathbb{R}^{3 \times 3} \text{ über } \mathbb{R}$$

aus?



Übersicht: Darstellung erzeugter Objekte

Struktur	Unterstruktur	Faktorstruktur
Gruppe ($G, +$)	Untergruppe. $E \subseteq G$ erzeugt $\left\{ \sum_{i=1}^n a_i \mid a_i \in \pm E \right\}$	Normalteiler. $E \subseteq G$ erzeugt $\left\{ \sum_{i=1}^n (g_i + a_i - g_i') \mid a_i \in \pm E, g_i \in G \right\}$
Ring ($R, +, \cdot$)	Unterring. $E \subseteq R$ erzeugt $\left\{ \sum_{i=1}^n \prod_{j=1}^{m_i} a_{ij} \mid a_{ij} \in \pm E \right\}$	Ideal. $E \subseteq R$ erzeugt $\left\{ \sum_{i=1}^n a_i \mid a_i \in \pm E U E U R E U R E U R E U R E \right\}$
Körper ($K, +, \cdot$)	Unterkörper. $E \subseteq K$ erzeugt $\left\{ \frac{\sum_{i=1}^n \prod_{j=1}^{m_i} a_{ij}}{\sum_{i=1}^o \prod_{j=1}^{\beta_i} b_{ij}} \mid a_{ij}, b_{ij} \in \pm E \right\}$	Nicht sinnvoll
Vektorraum ($V, +, \cdot$)	Unterraum. $E \subseteq V$ erzeugt $\left\{ \sum_{i=1}^n \alpha_i v_i \mid v_i \in E, \alpha_i \in K \right\}$	Unterraum
Modul ($V, +, \cdot$)	Unterm modul. $E \subseteq V$ erzeugt	Unterm modul
Algebra ($A, +, \cdot, \star$)	Unteralgebra. $E \subseteq A$ erzeugt	Algebra-Ideal

Polynome über Körpern

Größte gemeinsame Teiler in \mathbb{N} – Euklidischer Algorithmus

Definition

Für $n, m \in \mathbb{N}$ sind die Teiler $D(n, m) := \{t \in \mathbb{N} \mid t \mid n \wedge t \mid m\}$ und

$\text{ggT}(n, m) := k \in D(n, m)$, so dass $t \mid k \forall t \in D(n, m)$.

Man kann ihn durch Division mit Rest bestimmen. Z. B. für 98 und 35:

Größte gemeinsame Teiler in $K[t]$ – Euklid. Algorithmus

Definition

Für $p, q \in K[t]$ sind die Teiler $D(p, q) := \{d \in K[t] \mid d \mid p \wedge d \mid q\}$ und

$$\text{ggT}(p, q) := \{k \in D(p, q) \text{ höchsten Grades} \mid d \mid k \forall d \in D(p, q)\}.$$

Man kann sie durch Division mit Rest bestimmen. Z. B. für $p := t^3 - 1$ und $q := t^3 - t^2 + t - 1$ in $(\mathbb{R}[t], +, \cdot)$

Frage

Polynome werden über komm. Ringen mit Eins definiert und formen dann einen komm. Ring mit Eins. Wie sehen Polynome über Polynomen aus?

Polynome in mehreren Variablen

Frage

Wie könnte man Polynome in mehreren Variablen definieren?