Mathematik für Informatiker 1 – Tutorium

Malte Isberner

30.1.2014

Thema heute

Thema heute: Algebra (Teil 3)

- Kern
- Faktorstrukturen (für Ringe)
- Homomorphismen (für Ringe/Körper)
- Vektorräume

Kern und Normalteiler

Wichtiger Begriff: Kern eines Homomorphismus $h\colon \langle G_1, \oplus_1\rangle \to \langle G_2, \oplus_2\rangle$:

$$\mathrm{Kern}(h) =_{df} \{a \in G_1 \mid h(a) = e_2\} = h^{-1}(e_2)$$

- Kern ist Normalteiler
- Homomorphiesatz: $G_1/\mathrm{Kern}(h)$ isomorph zu $\mathrm{Bild}(h)$.

Faktorstrukturen auf Strukturen mit zwei Verknüpfungen

- Frage: Lässt sich ein zu Normalteilern verwandtes Konzept auf Ringen $\langle R, \oplus, \odot \rangle$ etablieren?
- Antwort: Ja! Ideale

Ideale

Sei $\langle R, \oplus, \odot \rangle$ ein Ring und $I \subseteq R$. I heißt Linksideal von R gdw.

1. $\langle I, \oplus \rangle$ ist Untergruppe von $\langle R, \oplus \rangle$ ($\Rightarrow I \neq \emptyset$)
2. $\forall a \in I, r \in R.\ r \odot a \in I$ (alternativ: $\forall r \in R.\ r \odot I \subseteq I$)

analog dazu Rechtsideal ($\forall r \in R. I \odot r \subseteq I$).
I heißt Ideal von R ($I \lhd R$) gdw. I Links- und Rechtsideal

- Beobachtung: In kommutativen Ringen ist jedes Links- bzw. Rechtsideal automatisch ein Ideal
- Was folgt, falls $1 \in I$?
- Beispiel: $n\mathbb{Z} \lhd \mathbb{Z}$, $n \in \mathbb{N} \setminus \{0\}$

Faktorstrukturen

Analog zur Faktorgruppe (Nebenklassen der Normalteiler)

Faktorring

Sei $\langle R, \oplus, \odot \rangle$ ein Ring und $I \triangleleft R$. Dann bildet

$$R/I =_{df} \{a \oplus I \mid a \in R\} \qquad (a \oplus I =_{df} \{a \oplus i \mid i \in I\})$$

mit den Verknüpfungen

$$\begin{aligned} (a \oplus I) \oplus_I (b \oplus I) &=_{df} (a \oplus b) \oplus I \\ (a \oplus I) \odot_I (b \oplus I) &=_{df} (a \odot b) \oplus I \end{aligned}$$

einen Ring, den sog. Faktorring $\langle R/I, \oplus_I, \odot_I \rangle$

Homomorphismen

Ringhomomorphismus

Ein Ringhomomorphismus $h\colon \langle R, \oplus_R, \odot_R \rangle \to \langle S, \oplus_S, \odot_S \rangle$ ist strukturerhaltende Abbildung zwischen zwei Ringen:

$$\begin{aligned} h(a \oplus_R b) &= h(a) \oplus_S h(b) \\ h(a \odot_R b) &= h(a) \odot_S h(b) \end{aligned}$$

Spezialisierung „Ring-mit-1“-Homomorphismus: Ringhomomorphismus und zusätzlich $h(1_R) = 1_S$.

Auch hier: Klassifizierung (Ring-)Mono-, Epi-, Isomorphismus ($\langle R, \oplus_R, \odot_R \rangle = \langle S, \oplus_S, \odot_S \rangle$: (Ring-)Endo-, Automorphismus)

Analogien Normalteiler $\leftrightarrow$ Ideale

- $\langle \mathbb{Z}/n\mathbb{Z}, +_{n\mathbb{Z}}, \cdot_{n\mathbb{Z}} \rangle$ ist isomorph zu $\langle \mathbb{Z}_n, +_n, \cdot_n \rangle$
- Für $I \triangleleft R$ ist $f_I \colon R \to R/I$, $f_I(r) = r \oplus I$, ein Ringepimorphismus
- Für einen Ringhomomorphismus $h \colon R \to S$ ist Kern(h) ein Ideal

Besondere Ideale

Primideal

Sei R ein kommutativer Ring und $P \subset R$ ein Ideal von R. P ist ein Primideal von R gdw.

$$\forall a, b \in R.\ a \odot b \in P \Rightarrow a \in P \vee b \in P$$

Primideale und Nullteilerfreiheit

Sei R ein kommutativer Ring und $P \subset R$ ein Ideal von R. Dann ist P ein Primideal von R gdw. R/P nullteilerfrei ist.

Besondere Ideale

Primideal

Sei R ein kommutativer Ring und $P \subset R$ ein Ideal von R. P ist ein Primideal von R gdw.

$$\forall a, b \in R.\ a \odot b \in P \Rightarrow a \in P \vee b \in P$$

Primideale und Nullteilerfreiheit

Sei R ein kommutativer Ring und $P \subset R$ ein Ideal von R. Dann ist P ein Primideal von R gdw. R/P nullteilerfrei ist.

Zusatzbemerkung Nullteilerfreiheit

Der Begriff Körper war aufbauend auf den Integritätsbereich (d.h. Nullteilerfreiheit) definiert. Die Forderung, dass $\langle R \setminus \{0\}, \odot \rangle$ eine kommutative Gruppe ist, genügt aber bereits. (Warum?)

Vektorräume

Definition Vektorraum

Es sei $(K, +, \cdot)$ ein Körper. Eine Menge V heißt zusammen mit Verknüpfungen $+\colon V \times V \to V$ und $\cdot\colon K \times V \to V$ Vektorraum, wenn die folgenden Gesetze erfüllt sind:

1. $\langle V, + \rangle$ ist kommutative Gruppe
2. $1 \cdot \vec{v} = \vec{v} \quad \forall \vec{v} \in V$
3. $(s \cdot s') \cdot \vec{v} = s \cdot (s' \cdot \vec{v}) \quad \forall s, s' \in K, \vec{v} \in V$
4. $(s + s') \cdot \vec{v} = (s \cdot \vec{v}) + (s' \cdot \vec{v})$
5. $s \cdot (\vec{v} + \vec{w}) = s \cdot \vec{v} + s \cdot \vec{w}$

Wichtiger Unterschied zu Ringen: $\cdot$ ist keine innere Verknüpfung!

Vektorräume (Forts.)

Beispiele für Vektorräume:

- $\mathbb{R}^n$ bzw. dessen geometrische Interpretation: Pfeile im n-dimensionalen euklidischen Raum
- $K^{n\times m}$: $n \times m$-Matrizen über einem Körper K (für $n = m$ außerdem Ring mit Eins!)
- K^M: Funktionen, die von einer beliebigen Menge M in einen Körper K abbilden (mit stellenweiser Addition und Multiplikation)

Vektorräume (Forts.)

Beispiele für Vektorräume:

- $\mathbb{R}^n$ bzw. dessen geometrische Interpretation: Pfeile im n-dimensionalen euklidischen Raum
- $K^{n\times m}$: $n \times m$-Matrizen über einem Körper K (für $n = m$ außerdem Ring mit Eins!)
- K^M: Funktionen, die von einer beliebigen Menge M in einen Körper K abbilden (mit stellenweiser Addition und Multiplikation)

Strukturbetrachtungen (teilweise bekannt):

- Unterstruktur: Unterräume (oder Teilräume)
  - Schnitt erhält Unterraumeigenschaft!
  - Nachweis von Unterräumen: Abgeschlossenheit (bzgl. $+$ und $\cdot$)

Vektorräume (Forts.)

Beispiele für Vektorräume:

- $\mathbb{R}^n$ bzw. dessen geometrische Interpretation: Pfeile im n-dimensionalen euklidischen Raum
- $K^{n\times m}$: $n \times m$-Matrizen über einem Körper K (für $n = m$ außerdem Ring mit Eins!)
- K^M: Funktionen, die von einer beliebigen Menge M in einen Körper K abbilden (mit stellenweiser Addition und Multiplikation)

Strukturbetrachtungen (teilweise bekannt):

- Unterstruktur: Unterräume (oder Teilräume)
  - Schnitt erhält Unterraumeigenschaft!
  - Nachweis von Unterräumen: Abgeschlossenheit (bzgl. $+$ und $\cdot$)
- Homomorphismen: Lineare Abbildungen
  - Unterschied bei $\cdot$: $\varphi(s \cdot \vec{v}) = s \cdot \varphi(\vec{v})$
  - Kern einer linearen Abbildung: $\mathrm{Kern}(\varphi) = \varphi^{-1}(\vec{0})$
  - Kern ist (wie üblich) Unterstruktur (Unterraum)

Vektorräume (Forts.)

Beispiele für Vektorräume:

- $\mathbb{R}^n$ bzw. dessen geometrische Interpretation: Pfeile im n-dimensionalen euklidischen Raum
- $K^{n\times m}$: $n \times m$-Matrizen über einem Körper K (für $n = m$ außerdem Ring mit Eins!)
- K^M: Funktionen, die von einer beliebigen Menge M in einen Körper K abbilden (mit stellenweiser Addition und Multiplikation)

Strukturbetrachtungen (teilweise bekannt):

- Unterstruktur: Unterräume (oder Teilräume)
  - Schnitt erhält Unterraumeigenschaft!
  - Nachweis von Unterräumen: Abgeschlossenheit (bzgl. $+$ und $\cdot$)
- Homomorphismen: Lineare Abbildungen
  - Unterschied bei $\cdot$: $\varphi(s \cdot \vec{v}) = s \cdot \varphi(\vec{v})$
  - Kern einer linearen Abbildung: $\mathrm{Kern}(\varphi) = \varphi^{-1}(\vec{0})$
  - Kern ist (wie üblich) Unterstruktur (Unterraum)
- Rest- bzw. Nebenklassen, Faktorraum

Vektorräume (Forts.)

Beispiele für Vektorräume:

- $\mathbb{R}^n$ bzw. dessen geometrische Interpretation: Pfeile im n-dimensionalen euklidischen Raum
- $K^{n\times m}$: $n \times m$-Matrizen über einem Körper K (für $n = m$ außerdem Ring mit Eins!)
- K^M: Funktionen, die von einer beliebigen Menge M in einen Körper K abbilden (mit stellenweiser Addition und Multiplikation)

Strukturbetrachtungen (teilweise bekannt):

- Unterstruktur: Unterräume (oder Teilräume)
  - Schnitt erhält Unterraumeigenschaft!
  - Nachweis von Unterräumen: Abgeschlossenheit (bzgl. $+$ und $\cdot$)
- Homomorphismen: Lineare Abbildungen
  - Unterschied bei $\cdot$: $\varphi(s \cdot \vec{v}) = s \cdot \varphi(\vec{v})$
  - Kern einer linearen Abbildung: $\mathrm{Kern}(\varphi) = \varphi^{-1}(\vec{0})$
  - Kern ist (wie üblich) Unterstruktur (Unterraum)
- Rest- bzw. Nebenklassen, Faktorraum
- Neu: Lineare Unabhängigkeit, Basis, Dimension

Vektorräume – Typische Aufgaben

Beweise, dass eine Struktur einen Vektorraum bildet

Polynomräume

Es sei $K[X]$ die Menge der Polynome über einem Körper K. Ferner sei $V_n \subseteq K[X]$ die Menge aller Polynome über K, deren Grad durch $n \in \mathbb{N}$ beschränkt ist. Zeigen Sie: für alle $n \in \mathbb{N}$ bildet V_n mit der üblichen Addition sowie Skalarmultiplikation für Polynome einen Vektorraum

Beweise, dass eine Teilmenge einen Untervektorraum bildet

Ebenen-Unterräume

Es sei $V = \mathbb{R}^3$ und die Menge $U = \{(x, y, z)^t \in V \mid z = 0\} \subseteq V$ die xy-Ebene. Beweisen Sie, dass diese einen Untervektorraum von V bildet.

Vektorräume – Typische Aufgaben

Erzeugendensystem/Basis angeben:

Erzeugendensystem und Basis

- Welche Dimension hat der oben eingeführte Polynomraum V_n für ein festes $n \in \mathbb{N}$? Geben Sie eine Basis für V_n an.
- Ist $\{1+x, x+x^2, x^2+x^3, x^3+x^4, x^4+1\}$ ein Erzeugendensystem für V_4?

Lineare Abbildungen:

Lineare Abbildungen

V und $\mathbb{R}^2$ seien Vektorräume über $\mathbb{R}$, $f\colon V \to \mathbb{R}$ und $g\colon V \to \mathbb{R}$ seien lineare Abbildungen. Welche der folgenden Funktionen sind lineare Abbildungen?

1. $\varphi_1\colon \mathbb{R}^2 \to \mathbb{R}^2$, $\varphi_1(x,y) =_{df} (x \cdot y, x)$
2. $\varphi_2\colon \mathbb{R}^2 \to \mathbb{R}^2$, $\varphi_2(x,y) =_{df} (2x+y, y)$
3. $\varphi_3\colon V \to \mathbb{R}^2$, $\varphi_3(\vec{v}) =_{df} (f(\vec{v}), g(\vec{v}))$

Matrizen

$n \times m$-Matrix über einem Körper K ($n, m \in \mathbb{N}^+$): Schema der Form

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ & & \vdots & \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{pmatrix},$$

wobei $a_{ij} \in K$ für $1 \leq i \leq n, 1 \leq j \leq m$.

Matrix – Notation

- $A = (a_{ij})$
  - Achtung: nicht mit einzelnem Wert a_{ij} für feste i, j verwechseln!
  - Genauer: $A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}$
- Inhalt der i-ten Zeile, j-ten Spalte: A_{ij}
  - Achtung: Zwar ist $A_{ij} = a_{ij}$, aber A_{ij}-Notation ist allgemeiner
  - Beispiele: $(A + B)_{ij}$, $\left(A^{-1}\right)_{ij}$, $(A^t)_{ij}$

Matrizenmultiplikation

Matrizenmultiplikation

- Formal: $\cdot : K^{n\times m} \times K^{m\times k} \to K^{n\times k}$
- Das Ergebnis der Multiplikation einer $n \times m$ mit einer $m \times k$-Matrix ist eine $n \times k$-Matrix
  - Spezialfall $n = m = k$: quadratische Matrizen, $\cdot$ ist innere Verknüpfung $\Rightarrow$ Ring
  - Spezialfall $k = 1$: Matrix-Vektor-Multiplikation ($\Rightarrow$ Lineare Abbildungen)
- Definition: $(A \cdot B)_{ij} = \sum_{k=1}^{m} A_{ik} \cdot B_{kj}$
  - Skalarprodukt der i-ten Zeile mit der j-ten Spalte

Invertierung von Matrizen

n-dimensionale Einheitsmatrix (über K):

$$E^n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ & & \vdots & \\ 0 & 0 & \cdots & 1 \end{pmatrix},$$

es gilt $A \cdot E^n = E^n \cdot A = A$ für jede Matrix $A \in K^{n \times n}$
Achtung: Matrizenmultiplikation i.A. nicht umkehrbar
... aber falls zu A eine Inverse existiert, wird diese A^{-1} genannt (und A invertierbar oder regulär).

Invertierung von Matrizen (naiv)

Bestimmen Sie die Inverse zur Matrix $A = \begin{pmatrix} 1 & 6 \\ 2 & 4 \end{pmatrix}$ in $\mathbb{Z}_7$.

Invertierung von Matrizen: Gauß-Elimination

Gauß-Elimination: Verfahren zur Lösung linearer Gleichungssysteme

- Allgemeiner: Verfahren zur Invertierung von Matrizen
  - LGS: $A\vec{x} = \vec{b}$, also $\vec{x} = A^{-1}\vec{b}$
- Vorgehen: Umformung der Matrix A zu E^n durch Anwendung von Transformationsregeln
  - Transformationsregeln lassen sich selbst als Matrizen beschreiben, und deren Produkt ist A^{-1}

Invertierung von Matrizen (schwieriger)

Bestimmen Sie die Inverse zur Matrix $A = \begin{pmatrix} 1 & 3 & 0 \\ 4 & 0 & 2 \\ 5 & 6 & 3 \end{pmatrix}$ in $\mathbb{Z}_7$