Lineare Algebra II
3. Tutoriumsblatt

TECHNISCHE UNIVERSITÄT DARMSTADT

Fachbereich Mathematik
Prof. Jan H. Bruinier
Claudia Alfes
Markus Schwagenscheidt

Sommersemester 2013
29.05.2013

Gruppenübung

Aufgabe G1 (Einschränkungen sind diagonalisierbar)
Sei V ein endlichdimensionaler Vektorraum und $f : V \to V$ ein diagonalisierbarer Endomorphismus. Sei $W \subseteq V$ ein f-invarianter Unterraum, also $f(W) \subseteq W$. Dann ist $f|W$ diagonalisierbar.

Lösung: Seien $\lambda_1, \ldots, \lambda_k$ die Eigenwerte von f. Da diagonalisierbar ist, ist $\mathrm{Eig}(f, \lambda_i) = \mathrm{Hau}(f, \lambda_i)$ für alle $i = 1, \ldots, k$ nach einem Theorem aus der Vorlesung. Jeder Eigenwert von $f|W$ ist auch Eigenwert von f. Sei λ einer dieser Eigenwerte von $f|W$. Dann gilt

$$\mathrm{Eig}(f|W, \lambda) = \mathrm{Eig}(f, \lambda) \cap W,$$
$$\mathrm{Hau}(f|W, \lambda) = \mathrm{Hau}(f, \lambda) \cap W,$$

denn:

- Sei $v \in \mathrm{Eig}(f|W, \lambda)$. Dann ist $v \in W$ und $f(v) = f|W(v) = \lambda v$, also $v \in \mathrm{Eig}(f, \lambda) \cap W$. Sei umgekehrt $v \in \mathrm{Eig}(f, \lambda) \cap W$. Dann gilt $f|W(v) = f(v) = \lambda v$, also $v \in \mathrm{Eig}(f|W, \lambda)$.
- Sei $v \in \mathrm{Hau}(f|W, \lambda)$. Dann ist $v \in W$ und $(f|W - \lambda \mathrm{id}_W)^{m_i} v = 0$, wobei m_i die algebraische Vielfachheit von λ in P_f bezeichnet. Es gilt
$$(f - \lambda \mathrm{id}_V)^{m_i} v = (f|W - \lambda id_W)^{m_i} v = 0.$$
Dabei kann man f durch $f|W$ und id_V durch id_W ersetzen, da $v \in W$ ist. Es folgt $v \in \mathrm{Hau}(f, \lambda) \cap W$. Sei umgekehrt $v \in \mathrm{Hau}(f, \lambda) \cap W$. Dann gilt
$$(f|W - \lambda \mathrm{id}_W)^{m_i} v = (f - \lambda \mathrm{id}_V)^{m_i} v = 0$$
also $v \in \mathrm{Hau}(f, \lambda)$.

Damit gilt

$$\mathrm{Eig}(f|W, \lambda) = \mathrm{Hau}(f, \lambda) \cap W = \mathrm{Eig}(f, \lambda) \cap W = \mathrm{Hau}(f|W, \lambda)$$

für alle Eigenwerte λ von $f|W$. Nach dem Theorem ist $f|W$ diagonalisierbar.

Aufgabe G2 (Rechnen in $\mathbb{Z}/m\mathbb{Z}$)
Sei $m \in \mathbb{N}$. Wir definieren auf $\mathbb{Z}$ eine Äquivalenzrelation[1] durch

$$x \sim y \quad \Leftrightarrow \quad m \mid (x - y).$$

Statt $x \sim y$ schreibt man

$$x \equiv y \mod m.$$

Die Äquivalenzklassen bezeichnen wir mit

$$\overline{x} = \{y \in \mathbb{Z} : m \mid (x - y)\}$$

und nennen sie auch Restklassen modulo m. Die Menge aller Äquivalenzklassen notieren wir mit $\mathbb{Z}/m\mathbb{Z}$.

[1] Dass die Relation reflexiv und symmetrisch ist, ist klar. Zur Transitivität: Gilt $m|(x-y)$ und $m|(y-z)$, so ist $(x-z) = (x-y)+(y-z)$, also $m|(x-z)$).

(a) Beachte, dass die Elemente von $\mathbb{Z}/m\mathbb{Z}$ selbst Mengen sind, und keine Zahlen.

(b) Zwei Zahlen sind genau dann äquivalent modulo m (liegen in derselben Klasse), wenn sie bei Teilung durch m denselben Rest lassen.

(c) $\mathbb{Z}/m\mathbb{Z}$ enthält m Elemente. Als Repräsentanten kann man $\overline{0}, \ldots, \overline{m-1}$ wählen.

(d) Beispiel: $\mathbb{Z}/6\mathbb{Z}$. Wir haben die Repräsentanten $\overline{0}, \overline{1}, \ldots, \overline{5}$. Es gilt z.B. $13 \equiv -5 \equiv 1 \mod 6$ und $-9 \equiv 3 \mod 6$.

(e) Definiere Addition $+_m$ und Multiplikation $\cdot_m$ von Restklassen durch

$$\overline{x} +_m \overline{y} := \overline{x+y}, \quad \overline{x} \cdot_m \overline{y} = \overline{xy}.$$

Beachte, dass hier Mengen addiert und multipliziert werden. Warum ist das wohldefiniert (also unabhängig von den gewählten Repräsentanten x, y der Klassen $\overline{x}, \overline{y}$)?

(f) Beispiel: $\mathbb{Z}/5\mathbb{Z}$: Berechne $\overline{13} \cdot \overline{27} = \overline{3} \cdot \overline{2} = \overline{6} = \overline{1}$. Berechne $\overline{9057} \cdot \overline{10014} = \overline{2} \cdot \overline{4} = \overline{3}$. In modulo-Schreibweise haben wir z.B. $19 \cdot 36 \equiv 4 \cdot 1 \equiv 4 \mod 5$.

(g) Addition und Multiplikation auf $\mathbb{Z}/m\mathbb{Z}$ sind assoziativ, kommutativ und distributiv. $\mathbb{Z}/m\mathbb{Z}$ ist ein Ring.

(h) $\mathbb{Z}/m\mathbb{Z}$ hat Nullteiler, wenn m keine Primzahl ist, denn: Schreibe $m = ab$ mit echten Teilern a, b, dann ist $\overline{a} \cdot \overline{b} = \overline{m} = \overline{0}$. Beispiel: $2 \cdot 3 \equiv 0 \mod 6$, d.h. 2 und 3 sind nullteiler und somit auch nicht invertiebar in $\mathbb{Z}/6\mathbb{Z}$. Die Ausdrücke 2^{-1} oder $\frac{1}{2}$ machen in $\mathbb{Z}/6\mathbb{Z}$ keinen Sinn.

(i) $\mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p ist ein Körper, d.h. zu jedem $\overline{x} \in \mathbb{Z}/p\mathbb{Z}$, $\overline{x} \neq 0$, existiert ein $\overline{y} \in \mathbb{Z}/p\mathbb{Z}$ mit $\overline{x} \cdot \overline{y} = \overline{y} \cdot \overline{x} = \overline{1}$.
Denn: Euklidischer Algorithmus liefert y, z so dass $yx + zp = 1$, also $yx \equiv 1 \mod p$.
Schreiben $\overline{x}^{-1} := \overline{y}$, aber NICHT $\overline{y} = \frac{1}{\overline{x}}$.

(j) $(\mathbb{Z}/n\mathbb{Z})^*$ (manchmal auch $(\mathbb{Z}/n\mathbb{Z})^\times$) ist die Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$, also die Menge der invertierbaren Elemente.

Aufgabe G3 (Kleiner Satz von Fermat)
Sei $p \in \mathbb{N}$ eine Primzahl und $a \in \mathbb{Z}$ mit $p \nmid a$. Dann gilt

$$a^{p-1} \equiv 1 \pmod{p}.$$

Hinweise:

- Sie dürfen verwenden, dass die Ordnung einer Untergruppe die Gruppenordnung teilt (Erinnerung: Die Ordnung einer endlichen Gruppe ist gleich der Anzahl ihrer Elemente).

Lösung: Wir geben den Beweis stichpunktartig an:

- Da $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, ist die Einheitengruppe $(\mathbb{Z}/p\mathbb{Z})^* = (\mathbb{Z}/p\mathbb{Z}) \setminus \{\bar{0}\}$.
- $(\mathbb{Z}/p\mathbb{Z})^*$ ist abelsche Gruppe der Ordnung $p-1$.
- Wegen $p \nmid a$, gilt $\bar{a} \neq \bar{0}$ in $\mathbb{Z}/p\mathbb{Z}$.
- Die Folge $\bar{a}, \bar{a}^2, \bar{a}^3, \ldots$ wiederholt sich, d.h. es existieren i und j mit $1 \leq i \leq j$ und $\bar{a}^i = \bar{a}^j$, also ist $\bar{a}^{i-j} = \bar{1}$.
- Wähle ein n, welches minimal mit dieser Eigenschaft ist, also $\bar{a}^n = \bar{1}$ und $\bar{a}^i \neq \bar{1}$ für $i < n$.
  Dann sind $\bar{a}, \bar{a}^2, \ldots, \bar{a}^{n-1}, \bar{a}^n = \bar{1}$ paarweise verschieden und $H = \{\bar{1}, \bar{a}, \bar{a}^2, \ldots, \bar{a}^{n-1}\}$ ist eine Untergruppe von $\big((\mathbb{Z}/p\mathbb{Z})^*, \cdot\big)$.
  (Denn: $\bar{a}^i \cdot \bar{a}^j = \bar{a}^{i+j} = \bar{a}^r$, falls $i + j = qn + r$ mit $0 \leq r < n$, $\bar{a}^{-1} = \bar{a}^{n-1}$, $(\bar{a}^2)^{-1} = \bar{a}^{n-2}$ usw.)
- Nach dem Hinweis folgt, dass die Ordnung von H die Ordnung von $(\mathbb{Z}/p\mathbb{Z})^*$ teilt, also gilt $h = |H| \mid |(\mathbb{Z}/p\mathbb{Z})^*| = p-1$. Sei also $p - 1 = hq$ für ein $q \in \mathbb{N}$, dann gilt

  $$\bar{a}^{p-1} = (\bar{a}^h)^q = \bar{1}^q = \bar{1}.$$

  Also folgt, dass

  $$a^{p-1} \equiv 1 \pmod{p}.$$

Aufgabe G4 (Tipps zur Jordanschen Normalform)
Es sei A eine reelle oder komplexe $n \times n$-Matrix und λ ein Eigenwert von A.

- Grundvorraussetzung an A: Das charakteristische Polynom zerfällt in Linearfaktoren (dies ist für komplexe Matrizen stets erfüllt). Dann existiert die Jordan-Normalform von A.
- A und ihre Jordansche Normalform J sind ähnlich, d.h. es gilt $A = S^{-1}JS$ für eine geeignete Basiswechselmatrix J. Die zugehörige Basis, bzgl. derer A in Normalform J vorliegt, heißt Jordanbasis.
- $\dim(\mathrm{Hau}(f, \lambda))$ = algebraische Vielfachheit von λ im charakteristischen Polynom = Größe des Jordanblocks zu λ.
- Summe der Dimensionen der Haupträume = Summe der algebraischen Vielfachheiten = Grad des char. Pol. = Dimension des Vektorraums.
- geometrische Vielfachheit von λ = Anzahl der Jordan-Kästchen zu λ.