Proseminar Lineare Algebra: Themen

1. Lemma von Gauß und Kriterium von Eisenstein (2 Personen)

   Polynomring $\mathbb{Z}[x]$ ist faktoriell; Irreduzibilitätskriterien für Polynome in $\mathbb{Z}[x]$; Folgerungen für den Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen

   Artin, Algebra, Abschnitte 11.3 und 11.4

2. Matrixbüschel (2 Personen)

   Sei (A, B) ein Paar von $m \times n$ Matrizen über K. Wie kann man (A, B) durch simultane Umformungen ($PAQ = A_1$, $PBQ = B_1$) in eine einfachere Form bringen? Normalform für Matrixpaare? Evtl. Anwendung bei linearen impliziten Differential- bzw. Differenzengleichungen ($Bx(t+1) = Ax(t)$)

   Gantmacher, Matrizentheorie, Seite 372–387

3. Diagonaldominanz und Gerschgorin-Kreise (2 Personen)

   $A \in \mathbb{C}^{n \times n}$ heißt diagonaldominant, wenn $|a_{ii}| > \sum_{j \neq i} |a_{ij}|$; diagonaldominante Matrizen sind invertierbar; jeder Eigenwert von A liegt in einer der Kreisscheiben $\{\lambda \in \mathbb{C} \mid |\lambda - a_{ii}| \leq \sum_{j \neq i} |a_{ij}|\}$; allgemeinere Aussagen von ähnlichem Typ

   Gantmacher, Matrizentheorie, Seite 454–468

4. Lineare Codierungstheorie (2 Personen)

   Ziel: Versehe Nachricht mit Redundanz, damit Empfänger sie trotz Übermittlungsfehlern entziffern kann (z.B. ISBN-Code, CD-Player)

   Einführung in die Codierungstheorie, hauptsächlich lineare Codes und ihre Eigenschaften, Konstruktion spezieller Codes

   Willems, Codierungstheorie und Kryptographie, Seite 3–15 (Grundbegriffe, nur das Wichtigste überblicksmäßig) und Seite 15–26 (Schwerpunkt)

5. Decodierung von BCH-Codes (1 Person)

   Ziel: Bestimme zu einem empfangenen (verrauschten) Wort das Codewort, das eigentlich gesendet wurde (unter der Annahme, dass nicht allzu viele Fehler passiert sind). BCH-Codes sind eine Klasse von Codes, die z.B. die Reed-Solomon-Codes umfasst und bei der die Decodierung durch eine trickreiche Anwendung des erw. Euklidischen Algorithmus möglich ist.

   Willems (siehe oben), Seite 58–63

6. Primzahltests (2 Personen)

   Für viele Verfahren der Kryptographie braucht man große Primzahlen (mehrere Hundert Stellen). Wie testet man, ob eine Zahl prim ist oder nicht? Der simpelste Test basiert auf dem kleinen Satz von Fermat. Es gibt aber Zahlen, die diesen naiven Test recht gut überlisten (Carmichael-Zahlen).

Der Miller-Rabin-Test verfeinert den Fermat-Test und eliminiert damit das Problem der Carmichael-Zahlen. Ein weiterer probabilistischer Primzahltest stammt von Solovay-Strassen. Im Jahr 2002 wurde ein deterministischer Test gefunden (AKS-Primzahltest).

Willems (siehe oben), Seite 104–109 (Schwerpunkt) und 97–104 (Überblick)

7. Trägheitssatz von Sylvester und Kriterium von Hurwitz (2 Personen)

   Aus LA2 kennen Sie diverse Normalformen bzgl. der Ähnlichkeit bzw. Äquivalenz von Matrizen. Der Satz von Sylvester liefert eine Normalform bzgl. *Kongruenz* und erlaubt eine Klassifikation von symmetrischen Bilinearformen. Das Hurwitz-Kriterium ermöglicht eine konstruktive Bestimmung des Kongruenztyps einer Matrix. Insbesondere kann man damit rechnerisch entscheiden, ob eine Matrix pos. def. ist.

   Zerz, Skript zur LAII, Abschnitte 4.1 und 4.2

8. Quadriken (1 Person)

   Aus der Schule bekannt sind (vermutlich) die Kegelschnitte Ellipse, Hyperbel und Parabel. Alle sind Nullstellengebilde von quadratischen (d.h., Grad=2) Polynomen in 2 Variablen. Wie kann man an einem solchen Polynom systematisch erkennen, wie seine Nullstellenmenge aussieht? Wie lässt sich eine solche Klassifikation von der Ebene in den Raum fortsetzen (Ellipsoid, ein-/zweischaliges Hyperboloid etc.)?

   Zerz, Skript zur LAII, Abschnitt 4.4

9. Lineare Gruppen (1 Person)

   Klassische Matrixgruppen, wie sie in der Geometrie und Physik verwendet werden, insb. orthogonale Gruppen (Drehungen) und unitäre Gruppen (komplexes Analogon).

   Zerz, Skript zur LAII, Abschnitt 5.6 (basiert auf den Abschnitten 8.1, 8.2 in Artins Algebra)

Allgemeine Hinweise:

- Die Themen sind weitgehend voneinander unabhängig. Insbesondere müssen sie nicht in einer bestimmten Reihenfolge abgehandelt werden. (Aber 2 Personen, die zusammen ein Thema bearbeiten, sollten nach Möglichkeit beim selben Proseminartermin vortragen.)

- Einzige Ausnahmen: Thema 5 nach Thema 4. Sowohl Thema 8 als auch Thema 9 bauen auf Thema 7 auf (sind aber untereinander unabhängig).

- Bei allen Themen wird empfohlen, außer der angegebenen Primärquelle auch andere Literatur zu suchen und zu Rate zu ziehen.

- Die Themen für 2 Personen können ggf. im Umfang reduziert werden und so auch an eine Einzelperson vergeben werden.