Computer Algebra

Sebastian Iwanowski
FH Wedel

Vorbereitung für die Kapitel 7 - 9:
Algebraische Grundlagen

Referenzen zum Nacharbeiten und Wiederholen:

Demmig: Matrizen und Determinanten
Köpf 7.1-7.4
Folien Diskrete Mathematik Iw Kap. 4.5
Schulze-Pillot: Elementare Algebra und Zahlentheorie

Computer Algebra Grundlagen

Matrizen und Determinanten

- Matrizenoperationen: Addition und Multiplikation
- Zusammenhang zwischen Matrizen und Gleichungssystemen
- Zusammenhang zwischen Matrixrang und Lösbarkeit des Gleichungssystems
- Determinantenberechnung:
  Rekursive Entwicklung nach einer Zeile:
  $$\det(M) = (-1)^{i+1} a_{i1} \cdot \det(M_{i1}) + (-1)^{i+2} a_{i2} \cdot \det(M_{i2}) + \ldots + (-1)^{i+n} a_{in} \cdot \det(M_{in})$$
  Rekursive Entwicklung nach einer Spalte:
  $$\det(M) = (-1)^{1+i} a_{1i} \cdot \det(M_{1i}) + (-1)^{2+i} a_{2i} \cdot \det(M_{2i}) + \ldots + (-1)^{n+i} a_{ni} \cdot \det(M_{ni})$$
- Reguläre Matrizen und Zusammenhang zu Determinanten
- Gaussches Eliminationsverfahren und Anwendungen für Matrizen

Computer Algebra Grundlagen

Körper und Körpererweiterungen

Charakteristik von Körpern

- Definition: **Charakteristik eines Körpers** ist die kleinste Zahl $p \neq 0$ mit $p \cdot 1 = 0$ (falls existent, sonst 0)
- Satz: Endliche Körper haben eine Primzahl als Charakteristik.
- Satz: Unendliche Körper haben Primzahl als Charakteristik oder 0.

Dann enthält der Körper als kleinsten Körper die gebrochen rationalen Funktionen über $\mathbb{Z}_p$

Dann ist $\mathbb{Q}$ als kleinster Körper enthalten.

Körper und Körpererweiterungen

Algebraische Körpererweiterungen und ihre Darstellung mit Polynomen und Vektorräumen

- Definition: Sei α eine Nullstelle des Polynoms $p(x) \in K[x]$. Dann heißt α eine **algebraische Zahl** für K und **K(α)** ist der kleinste **Erweiterungskörper** von K, der α enthält.
- Definition: Ein Element τ eines Erweiterungskörpers von K, das von keinem Polynom aus K[x] Nullstelle ist, heißt **transzendent**.
- Definition: Gegeben eine algebraische Zahl α für K. Dann ist das **Minimalpolynom** $p_\alpha(x) \in K[x]$ das Polynom minimalen Grades, das α als Nullstelle hat.
- Satz: Jedes **Minimalpolynom** einer algebraischen Zahl **ist irreduzibel**.
- Satz: Wenn das Minimalpolynom von α den Grad n hat, dann ist $K(\alpha)$ isomorph zu dem Körper aller Polynome vom Grad maximal n-1. Gerechnet wird in $K(\alpha)$ mit der üblichen Polynomaddition und Polynommultiplikation modulo $p_\alpha(x)$.
- Satz: Wenn das Minimalpolynom von α den Grad n hat, dann ist $K(\alpha)$ bezüglich der Addition isomorph zu einem Vektorraum der Dimension n über K.

Computer Algebra Grundlagen

Körper und Körpererweiterungen

Algebraische Körpererweiterungen und ihr Abschluss

- Definition: Ein Körper, der durch die Hinzunahme von endlich vielen algebraischen Elementen aus K gebildet wird, heißt **endliche Körpererweiterung** von K. Der Grad n dieser Körpererweiterung ist der kleinste Grad eines Polynoms, das jede der hinzugenommenen Elemente als Nullstelle enthält.

  Satz: Ein solches existiert immer.

- Satz: Zu jedem Polynom aus K[x] gibt es eine endliche Körpererweiterung, in der das Polynom in n Linearfaktoren zerfällt. Der Grad dieser Körpererweiterung ist ein Teiler von n.
- Definition: Die kleinste Körpererweiterung, in der ein Polynom p(x) in Linearfaktoren zerfällt, heißt **Zerfällungskörper von p**.
- Definition: Der **algebraische Abschluss** eines Körpers ist der Körper, in dem alle Polynome aus K[x] in Linearfaktoren zerfallen. Er enthält also alle Zerfällungskörper.
- Beispiel: Der Körper $\mathbb{C}$ ist der algebraische Abschluss von $\mathbb{R}$. Er hat den Erweiterungsgrad 2.
- Satz: Alle unendlichen Körper mit Charakteristik 0 sind in $\mathbb{C}$ enthalten.
- 2. Beispiel: Der algebraische Abschluss von $\mathbb{Q}$, der alle algebraischen Elemente über $\mathbb{Q}$ enthält, ist eine **unendliche, aber abzählbare** Körpererweiterung.