3.3.1 Computeralgebra in der Informatik

In vielen Teilgebieten der Informatik können Techniken der Computeralgebra zur Lösung wichtiger Fragestellungen eingesetzt werden.

Verwendet werden beispielsweise Strukturen zur Darstellung mathematischer Zusammenhänge (z.B. Formeln) und Werkzeuge zur Inferenz auf diesen Wissensbasen für *wissensbasierte Systeme für die Mathematik* (s. 2.15, 2.19).

Die Algebra stellt eine der Grundlagen der *Codierungstheorie* und *Kryptographie* dar; sowohl algebraische Algorithmen als auch Computeralgebra-Systeme lassen sich beim Entwurf und der Modellierung von Übertragungssystemen, Sicherheitsmechanismen und Protokollen einsetzen. Moderne Ansätze sind durch die Benutzung algebraischer (insbesondere elliptischer Kurven) entstanden, sowie durch dir Enge Verknüpfung klassischer algebraischer Methoden im *VLSI-Entwurf* sowie in der methodischen Entwicklung *effizienter Algorithmen*, wie dies am Beispiel der schnellen Fourier-Transformationen und parallelen Algorithmen deutlich wird (s. 2.3, 2.17).

Weitere Anwendungsbeispiele findet man bei der *automatischen Formelmanipulation* in Relationenalgebren sowie beim Lösen von Entscheidungsproblemen in algebraischen Strukturen durch *Termersetzungs- und Reduktionssysteme* (s. 2.13.1). Wichtige Hilfsmittel beim *automatischen Beweisen* werden durch Gröbnerbasen und charakteristische Mengen bereitgestellt (s. 2.6).

Computeralgebra-Algorithmen werden darüber hinaus erfolgreich für die *Verbands- und Ordnungstheorie* mit Anwendungen auf Datenanalyse und Wissensrepräsentation, *Testbeispiele* für neuartige parallele und verteilte Rechnersysteme sowie in der *Automatentheorie* (s. 8.3.8) eingesetzt.

Thomas Beth und Karsten Homann (Karlsruhe)